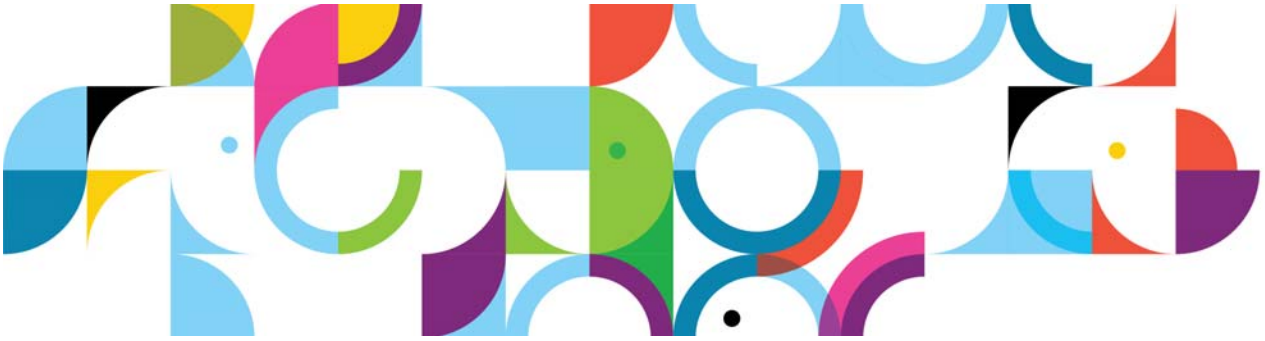
IBM Connections 4 Public Deployment Scenarios

Deployment Scenarios

ERC 1.0



Trademarks

IBM® and the IBM logo are registered trademarks of International Business Machines Corporation.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

AIX®	Cognos®	DB™
DB2 Universal Database™	DB2®	Domino®
Lotus®	LotusScript®	Notes®
Power®	Quickr®	Rational®
Sametime®	System z®	Tivoli®
WebSphere®	400®	

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

January 2013 edition

IBM Connections 4: How to Deploy a Two Node Cluster of IBM® Connections V4.0 configured with SPNEGO security, on Red Hat Server (RHEL) x86-64, 6.3

About the author

Patrick (Pat) Cadogan has worked with IBM for over 25 years. Pat initially started working at Lotus Development (Sep 1986), and focused on the globalization and localization of Lotus products (including Lotus 1-2-3, Freelance, Symphony, Improv, and Lotus Notes/Domino). In 1995, IBM acquired Lotus; in 1998, Pat moved to the IBM Lotus lab in Massachusetts, US, where he worked on Lotus Domino for Linux, iSeries, and zSeries. After five years in the US, Pat returned home to the IBM Dublin Lab where he has focused on System Verification Testing of various IBM products, including Lotus Quickr Java Platform, Enterprise Edition, and IBM Connections V2x, 3x, and now V4. Pat can be reached at pcadogan@ie.ibm.com.

Reference

- IBM Connections V4.0 announcement:

  http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/5/760/ENUSJP12-0265/index.html&lang=en&request_locale=en

- Hardware and software requirements:

  http://www-01.ibm.com/support/docview.wss?uid=swg27012786

- IBM Connections 4 product documentation:

  http://www-10.lotus.com/ldd/lcwiki.nsf/xpViewCategories.xsp?lookupName=Product%20Documentation

- Tutorial - Installing IBM Connections 4.0 on a Linux RHEL 6.3 64 bit system:

  http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Tutorial_-_Installing_IBM_Connections_4.0_on_a_Linux_RHEL_6.3_64-bit_systemcol

Contents

1. Deployment topology

2. IBM Connections 4 system requirements

3. Middleware installation and configuration steps (WebSphere Application Server v7.0.0.21 / IBM HTTP Server v7.0.0.21 / DB2 v9.7+FP6 / Tivoli Directory Integrator v7.1+FP5)

4. Create Connections databases on DB2 server by using the dbWizard

5. Populate the Profiles database with LDAP user information

6. Installation of IBM Connections v4.0

7. Post-IBM Connections installation steps

8. Configuring SPNEGO

1. Deployment topology

Install IBM® Connections 4.0 in a network deployment to achieve optimum scaling, load balancing, and failover.

A network deployment can consist of a single server with all applications installed, or two or more sets of servers that are grouped to share the workload. You must also configure an additional system with WebSphere® Application Server Network Deployment Manager, which you can use to build, manage, and tune the clustered servers.

A network deployment provides the administrator with a central management facility, and it ensures that users have constant access to data. It balances the workload between servers, improves server performance, and facilitates the maintenance of performance when the number of users increases. The added reliability also requires a larger number of systems and the experienced administrative personnel who can manage them.

Standard Enterprise Network Deployment Architecture

Figure 1, "Standard enterprise network deployment architecture," on page 3 shows the enterprise-level network deployment of IBM Connections 4.0 without any additional complexity. This topology shows a two-node cluster of IBM Connections, in which the LDAP and database servers communicate with the cell controlled by the Deployment Manager. The Tivoli Directory Integrator server sits between the database and LDAP, maintaining synchronization between both.

IBM Connections is installed on the Deployment Manager server and from there is pushed out to the nodes in the cell: node01Node and node02Node. The shared data store is a shared space accessible from all nodes in the configuration and the Deployment Manager. In this case, the shared space is mounted on the Deployment Manager server and shared with both nodes, at the same location on those servers.

Sitting in front of the entire configuration is the web server, from which the user accesses IBM Connections 4.0.

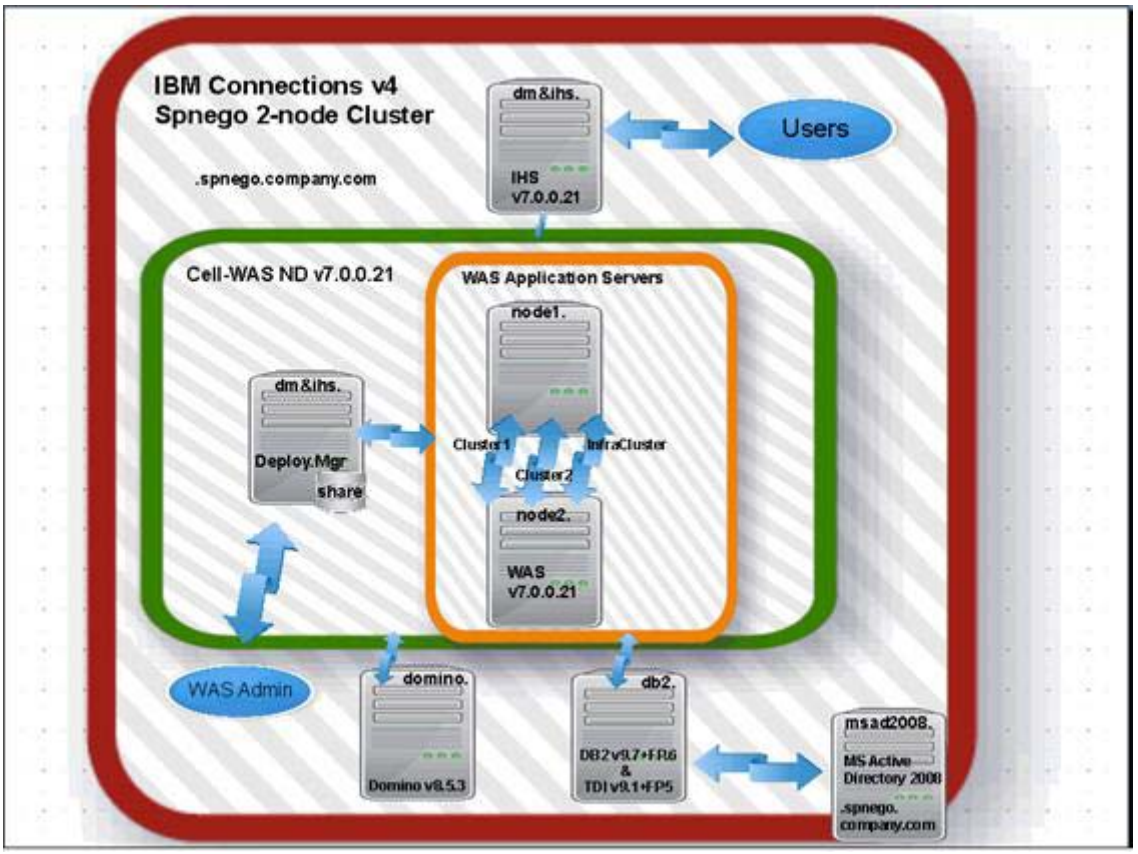


Figure 1. Standard enterprise network deployment architecture

Note

Notes for this topology diagram:

- Cognos/Metric is not installed.
- The WebSphere Application Server Deployment Manager and the IBM HTTP Server both coexist on the same physical server, but they are depicted (in the diagram) as existing on different servers. This depiction is to help simplify understanding of this deployment; the host name is the same for both.
- The Domino Mail-In server is not integrated with the MS-AD2008 LDAP so that users are not automatically created as needed on the Domino mail server. Instead, Domino Mail-In users were created manually (as needed) and the mapping between IC4 and Domino users was based on the user's email address. This is not typically how customers would configure Notifications and Domino mail integration.

When you install IBM Connections 4.0, there are three deployment options to choose from: small, medium, and large. This deployment uses the Medium topology.

Topology: **Medium** deployment

Install a subset of applications in separate clusters. IBM Connections provides three predefined cluster names that are shared among all 12 applications. Use this option to distribute applications according to your usage expectations. For instance, you might anticipate higher loads for the Profiles application and install it in its own cluster, while other applications might be installed in a different cluster. With this option, you can maximize the use of available hardware and system resources to suit your needs.

2. IBM Connections 4 system requirements

See product documentation: `http://www-01.ibm.com/support/docview.wss?uid=swg27035893`, which covers supported operating systems, databases, software integration, browsers, and so on..

Table 1: Systems specification that is used in this deployment

Server host name	Application	Version number	OS/version	HW / RAM / CPU / HDD
dm&ihs.spnego.company.com	• WebSphere Application Server Deployment Manager • IBM HTTP Server	• WebSphere Application Server v7.0.0.21 (64-bit) • IBM HTTP Server v7.0.0.21	RedHat 6 (64 bit) Enterprise	VM / 8 GB / 2 CPUs / 80 GB
node1.spnego.company.com	• Node1 (WebSphere Application Server)	• WebSphere Application Server v7.0.0.21		VM / 8 GB / 2 CPUs / 80 GB
node2.spnego.company.com	• Node2 (WebSphere Application Server)	• WebSphere Application Server v7.0.0.21		VM / 8 GB / 2 CPUs / 80 GB
db2.spnego.company.com	• DB2 • Tivoli Directory Integrator	• DB2 v9.7+FP6 • Tivoli Directory Integrator v7.1+FP5		VM / 8 GB / 2 CPUs / 80 GB
msad2008.spnego.company.com	• MS Active Directory 2008	• 2008	Win2008 R2 EE Server	
domino.company.com	• Domino Mail-In server	• Domino 8.5.3	Win2008 R2 EE Server	VM / 4 GB / 2 CPUs / 40 GB

The following examples for installing IBM Connections 4 use a fictitious user called **AdminFromLDAP**. This user must meet the following criteria:

- Is a valid user from the LDAP used in this Connections deployment
- Is populated to the Profiles database when the population tool is run
- Is granted Admin access to the Deployment Manager so that this user can log in to the WebSphere Application Server console and can administer all aspects of Connections
- Is selected as the Connections administrator when the user runs the Connections installation wizard.

Critical patches for WebSphere and RedHat 6 required before IBM Connections 4 is installed

a. **Linux RedHat 6 (64-bit) OS essential patches**: See the IBM Connections information center for details:

   `http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Linux_libraries_ic40&content=pdcontent`

b. **WebSphere 7.0 with FixPack 21 is the minimum requirement.**

c. **Required WebSphere interim fixes to install on top of WebSphere Application Server 7-FixPack 21:**

   - PM53930: WebSphere Application Server Java HashTable security fix
   - PM56596: WebSphere Application Server JMS/SIB fix for messages that build up
   - PM60895: WebSphere Application Server JMS/SIB fix for pending messages not cleaning up at end points
   - PM51981: Fixes issues if you upgrade WebSphere from FixPack 19: 21
   - PM65486: OAuth Provider interim fix that is published for WebSphere Application Server FP 7.0.0.21

d. **Synchronize the time on all systems** in the deployment by running: **ntpdate clock.redhat.com** on each system.

e. **Configure the Open File Descriptor limit to at least 8192 on all systems (Deployment Manager, Node1, Node2, and DB2)**

   `vi /etc/profile`

   Add **`ulimit -n 8192`**

   Verify by running: **`ulimit -a`**

   On non-Windows platforms, ensure that the Open File Descriptor limit is set to at least 8192:

   `ulimit -n 8192`

f. **Set up an NSF4 Shared Area for the Deployment Manager, Node1, and Node2**

   - In a multinode clustered environment, it is necessary to set up a shared area which all nodes access.
   - All nodes in the cluster must have read and write access to this area.
   - This access is used to store indexes which Connections needs.
   - This area must be set up before the Connections installation because the installation asks for this location during the setup process.

Note

Use a 'fast reliable networked file system' for both this shared file area and the server were you locate your databases.

When you use NFS, use NFS v4, because NFS v3 lacks advanced locking capability.

On Linux, an easy way is to set up an NFS share on a server (such as your Deployment Manager) and then map to this share (folder) from each node.

Follow these steps to do it:

On the Deployment Manager system, create a Share folder (by using NFS4 Server):

- Create a folder on the system you want to share the folder on. For example, on the Deployment Manager system, create a folder `/opt/IC_Share` such as: **`mkdir /opt/IC_Share`**
- Give full read/write access to this folder: **`chmod -R 755 /opt/IC_Share`**

  With NFS v4 you can export just one file system, so all the folders you need to mount on the clients must be under this one.
- Edit the `/etc/exports` file (**`#vi /etc/exports`**) and add the following lines:

  ```
  /opt/IC_Share   node1.company.com(rw)
  /opt/IC_Share   node2.company.com(rw)
  ```
- Write and quit `:wq!`
- Verify that the **nsf** service is running. If it is not, then enable it with services:

  ```
  service nfs restart | stop | start
  mount -all
  ```

You now shared this folder to systems node1 and node2.

Configure Node1 and Node2 to access the shared folder on the Deployment Manager system as follows:

- Enable the **nfs** service on node1 and node2.
- Create the folder to mount to, such as: **`mkdir /opt/IC_Share`**
- Add the following line to:

  ```
  vi /etc/fstab
  dm&ihs.spnego.company.com:/opt/IC_Share   /opt/IC_Share  nfs
  ```

  - Mount the remote file system: **`mount -all`**

3. Middleware installation and configuration steps (WebSphere Application Server v7.0.0.21 / IBM HTTP Server v7.0.0.21 / DB2 v9.7+FP6 / Tivoli Directory Integrator v7.1+FP5)

Summary steps:

- Install WebSphere Application Server V7.0 Deployment Manager on system `dm&ihs.spnego.company.com`
- Install WebSphere Application Server V7.0 Application Server on `node1.spnego.company.com`
- Install WebSphere Application Server V7.0 Application Server on `node2.spnego.company.com`
- Install IBM HTTP Server V7.0 web server on `dm&ihs.spnego.company.com`
- Update Deployment Manager, Node1, Node2 IBM HTTP Server, IBM HTTP Server Plugin, and SKD to WebSphere Application Server V7 Fixpack 21
- Federate Application Servers (node1 and node2) into the Deployment Manager
- Enable Security on the Deployment Manager
- Install DB2 server V9.7-Fixpack 6 on `db2.spnego.company.com`
- Apply the DB2 License to the DB2 server
- Install and Configure Tivoli Directory Integrator V7.1 (Tivoli Directory Integrator) on db2.spnego.company.com
- Upgrade Tivoli Directory Integrator V7.1 to Fixpack 5

Note

All systems must be part of the SPNEGO domain that is defined in the MS Active Directory 2008; this document referred to the SPNEGO domain as **spnego.company.com**.

In this scenario, you install the WebSphere Application Server Deployment Manager (Deployment Manager) and the IBM HTTP Server (IBM HTTP Server) on the same system called **dm&ihs.spnego.company.com**.

Install IBM WebSphere Deployment Manager: 7.0.0.0

1. Copy the WebSphere Application Server 7.0 setup image `C1G35ML.tar.gz` to your Deployment Manager server; extract and go to the `WebSphere Application Server` folder.
2. Start the Deployment Manager installer by running **install** from within the `WebSphere Application Server` folder. You see the following panel. Click **Next** to continue.

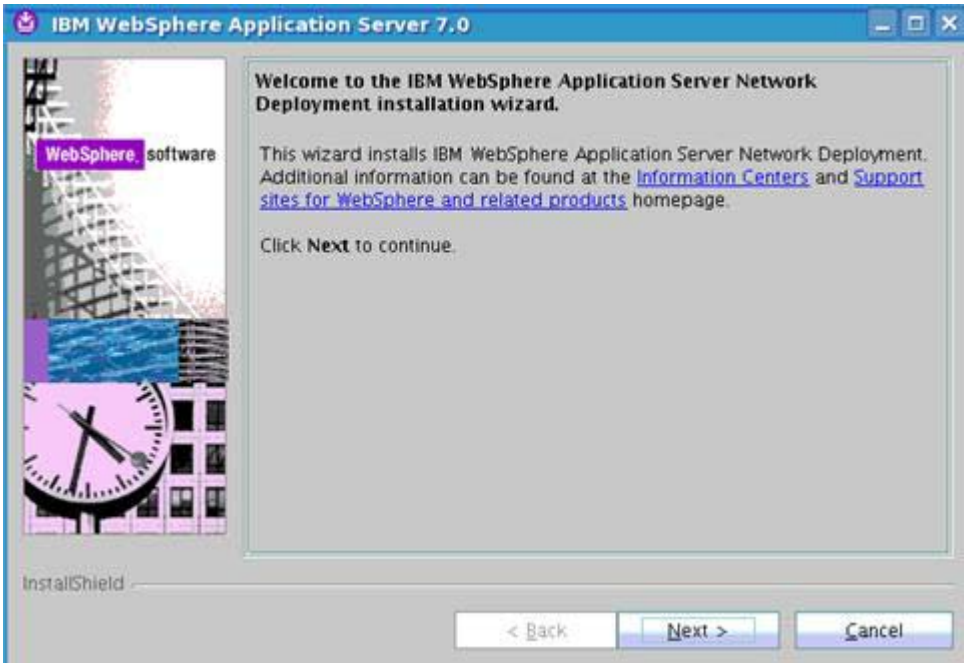


Figure 2. IBM WebSphere Application Server 7.0 installation welcome screen

__ 3. Accept the license agreement. Click **Next**.

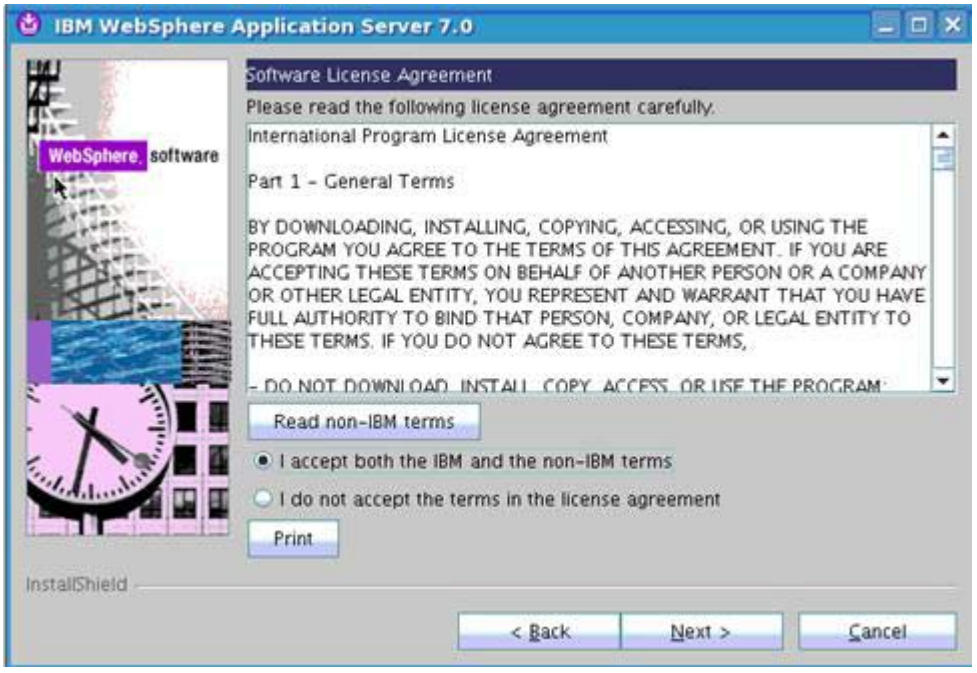


Figure 3. IBM WebSphere Application Server 7.0: Software license agreement

__ 4. In the System Prerequisites Check panel, click **Next**.

Figure 4. IBM WebSphere Application Server 7.0: System Prerequisites Check

__ 5. Do not select any options from the Optional Features Installation. Click **Next** to continue.

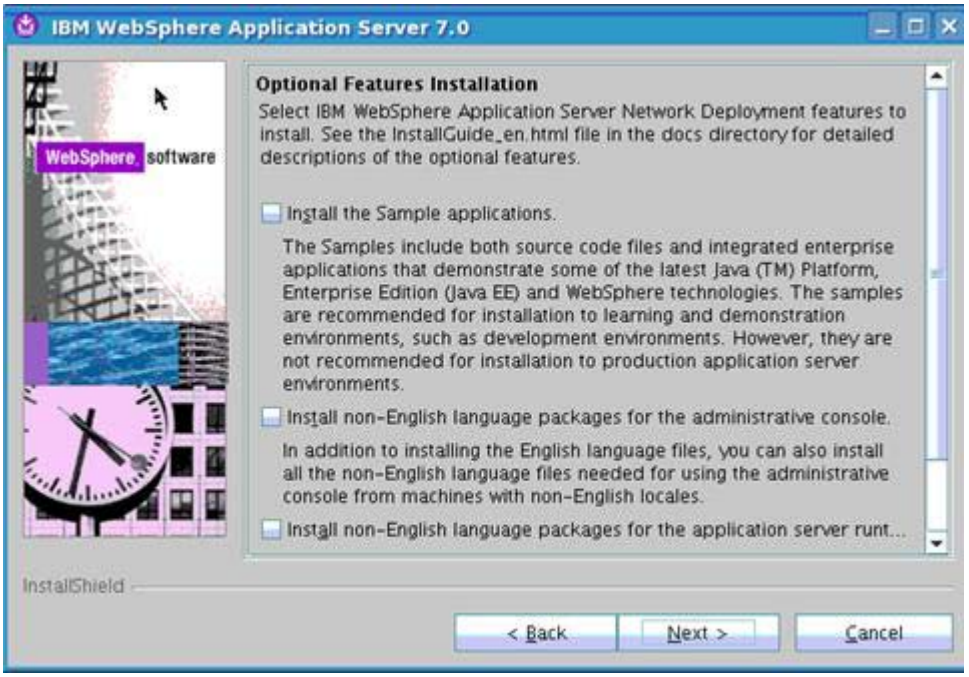


Figure 5. IBM WebSphere Application Server 7.0: Optional Features Installation

__ 6. Change the default installation path if necessary. Otherwise, use the default location `/opt/IBM/WebSphere/AppServer`.

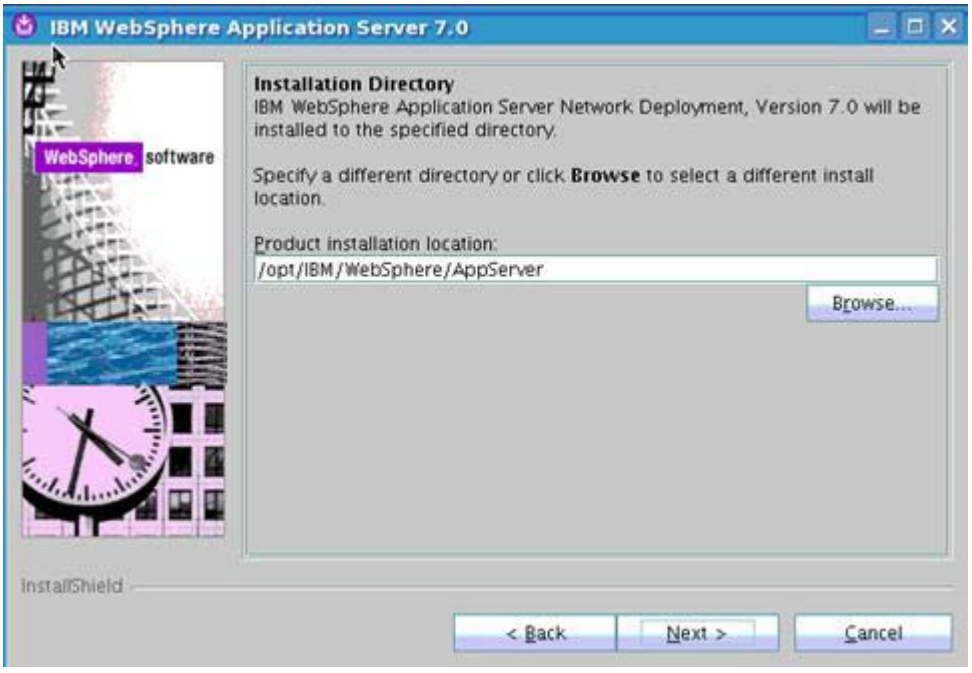


Figure 6. IBM WebSphere Application Server 7.0: Installation Directory

__ 7. Select **Management** (to install the deployment manager).

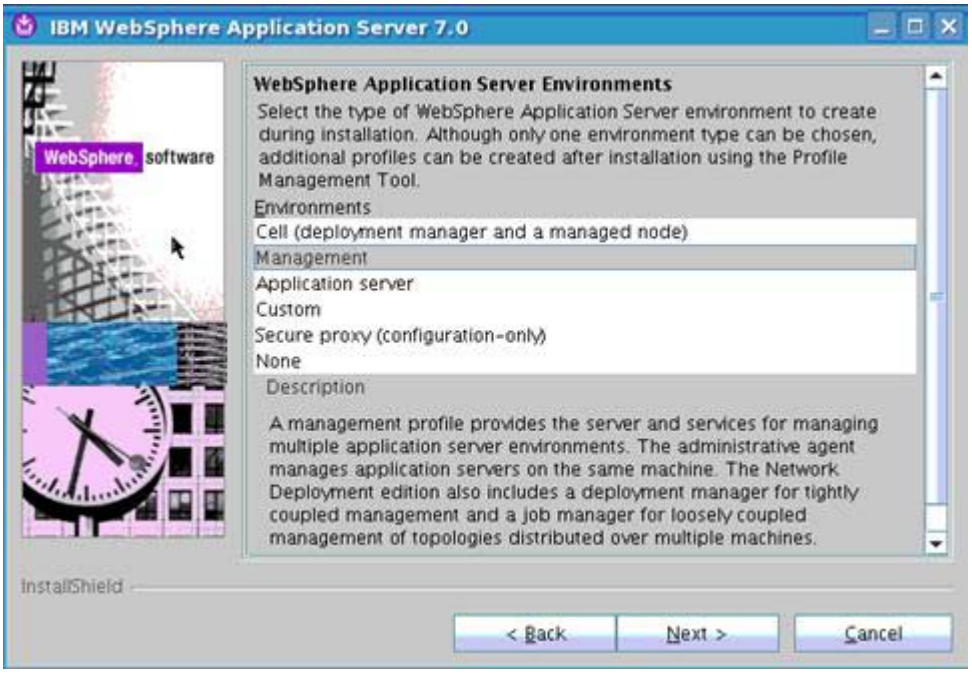


Figure 7. IBM WebSphere Application Server 7.0: WebSphere Application Server environments

__ 8. Select **Deployment Manager**.

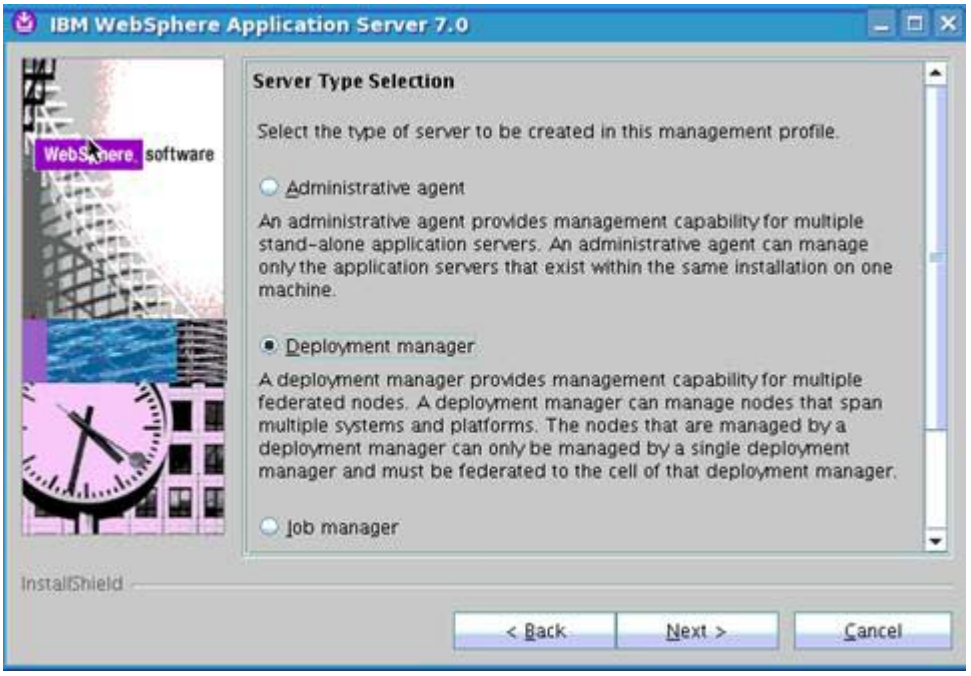


Figure 8. IBM WebSphere Application Server 7.0: Server Type Selection

__ 9. Enter the user name and password.

Figure 9. IBM WebSphere Application Server 7.0: Enable Administrative Security

__ 10. Do not select the **Create a repository** option.

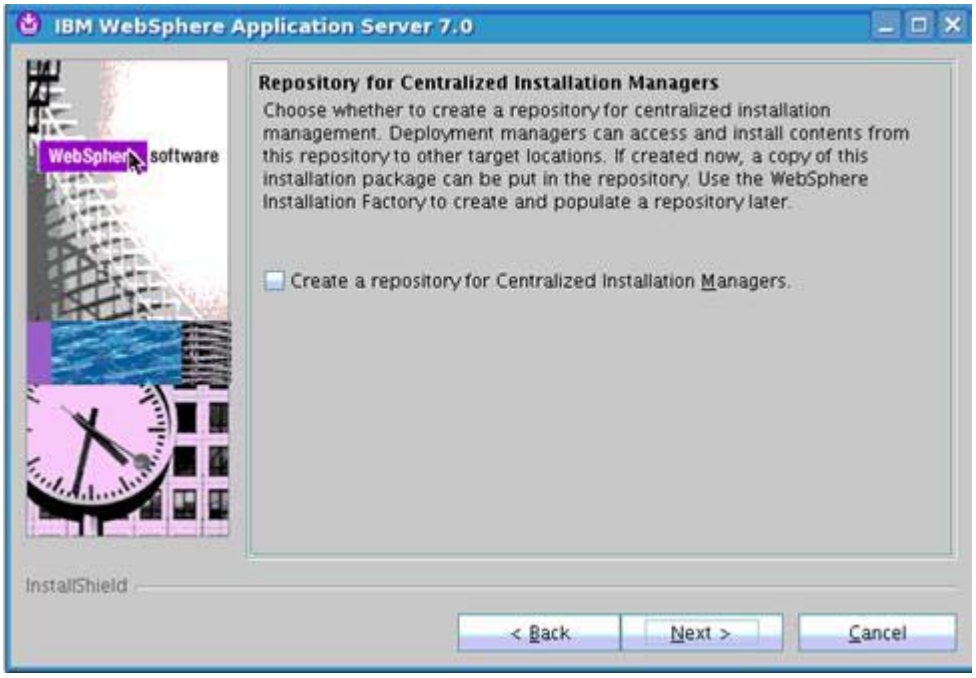


Figure 10. IBM WebSphere Application Server 7.0: Repository for Centralized Installation Managers

__ 11. Select the "Verify my permissions" option. Click **Next**.

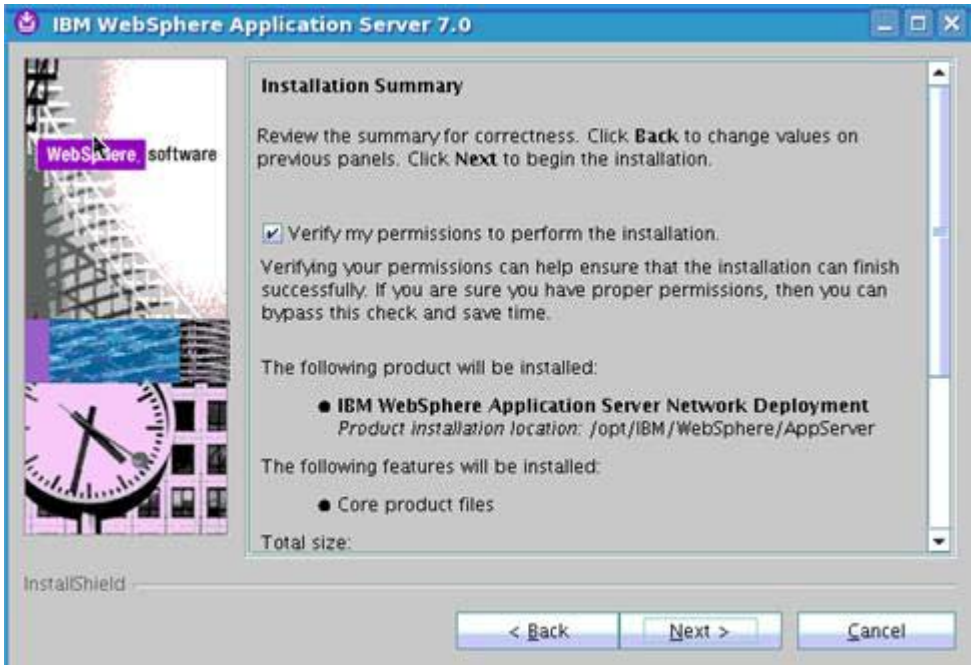


Figure 11. IBM WebSphere Application Server 7.0: Installation Summary

__ 12. Click **Next**.

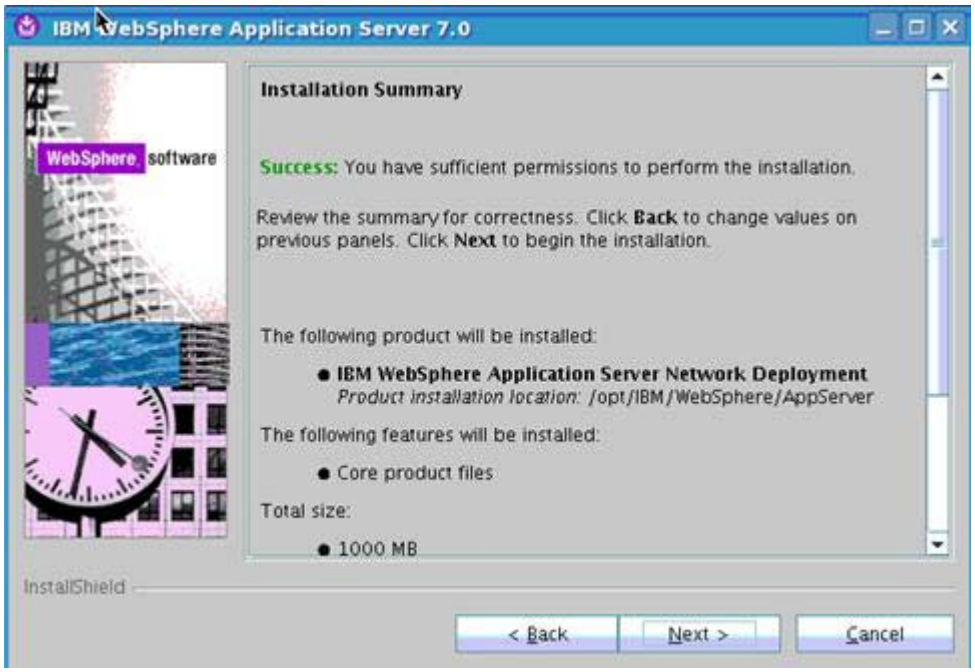


Figure 12. IBM WebSphere Application Server 7.0: Installation Summary

The installation starts to copy files.

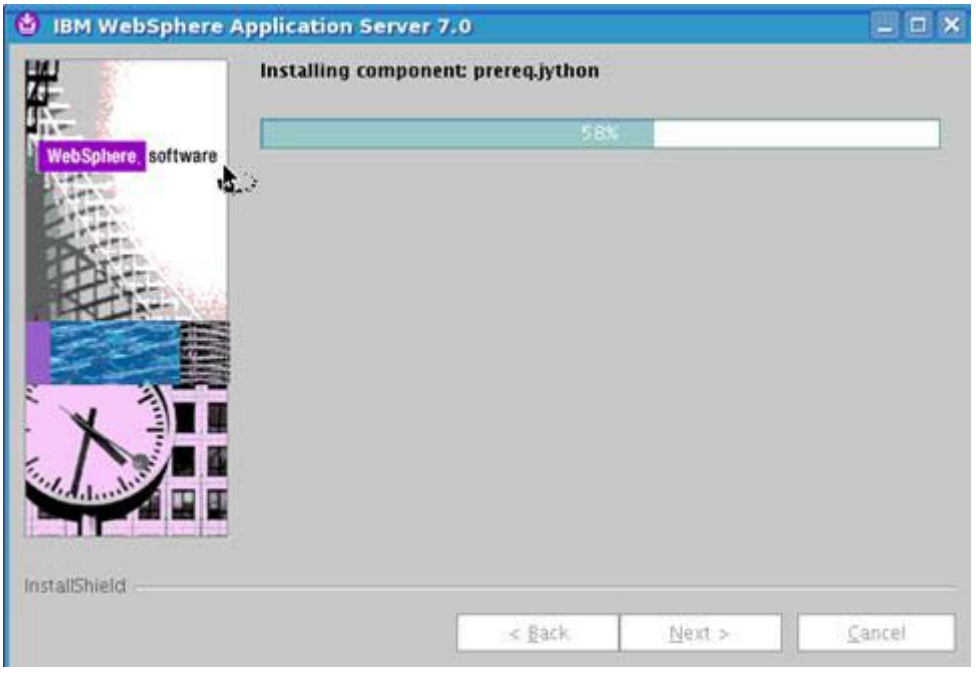


Figure 13. IBM WebSphere Application Server 7.0: Installation in progress

__ 13. After some time the installation finishes. Click **Finish** to exit the installer.

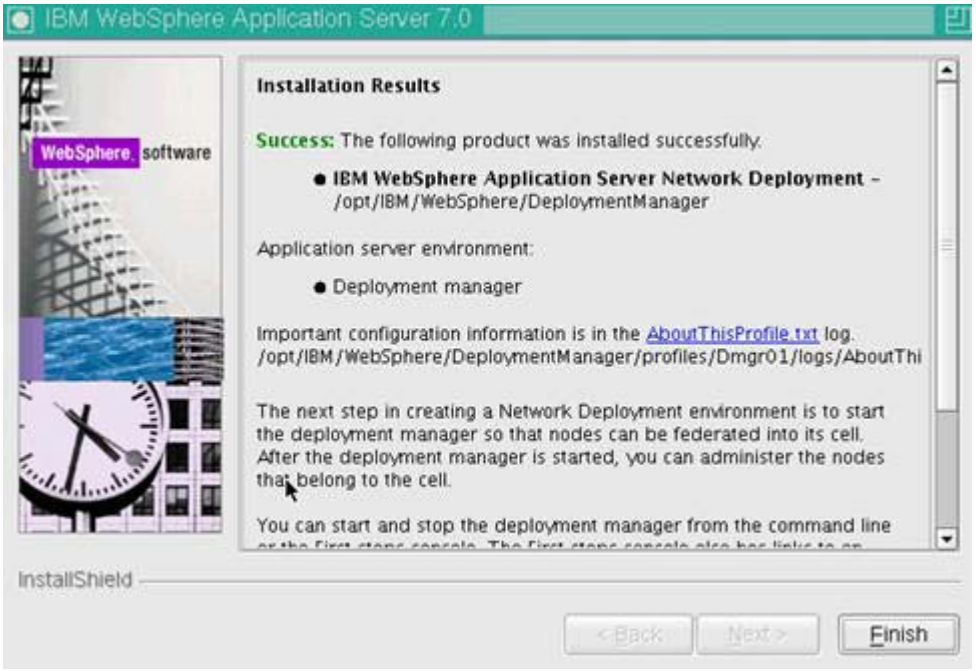


Figure 14. IBM WebSphere Application Server 7.0: Installation results: Success

__ 14. You return to this screen. Click **Installation Verification**.

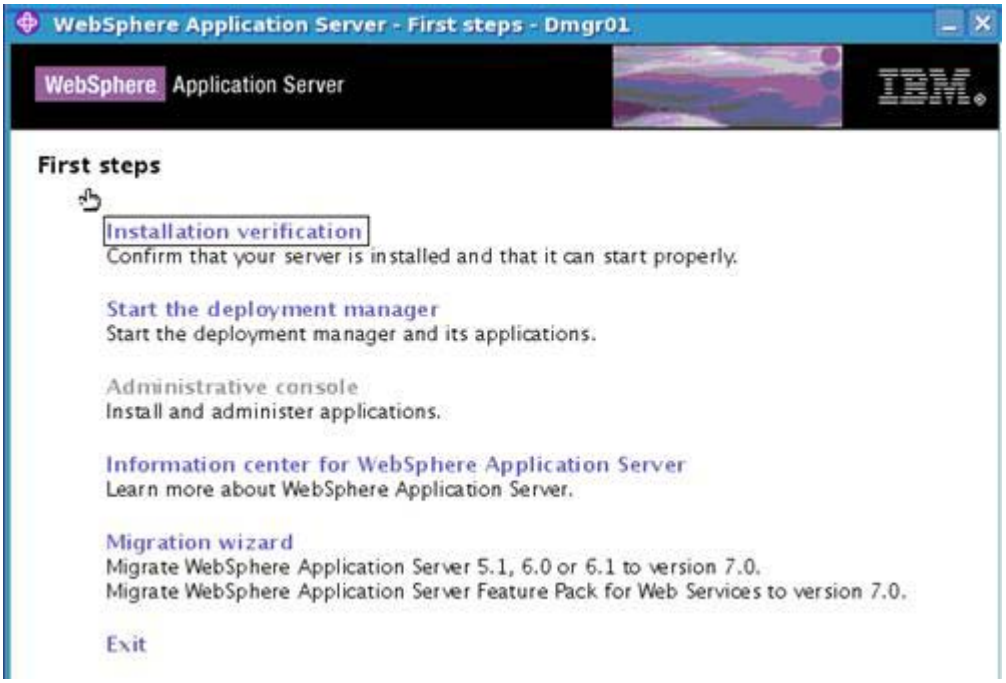


Figure 15. WebSphere Application Server: First steps screen

The Deployment Manager is now set up. Here is the output.

Figure 16. First steps output: Installation verification

Install IBM WebSphere Application Server: 7.0.0.0

Note

Do this step on each node of your deployment configuration.

In this document, we install and configure two nodes called:

- `node1.spnego.company.com`
- `node2.spnego.company.com`

__ 15. Copy the WebSphere Application Server 7.0 setup image `C1G35ML.tar.gz` to your Node 1 and Node 2 computers and start the Application Server installer by running `install` from within the `WebSphere Application Server` folder. You should see the screen like in the following figure. Click **Next** to continue.

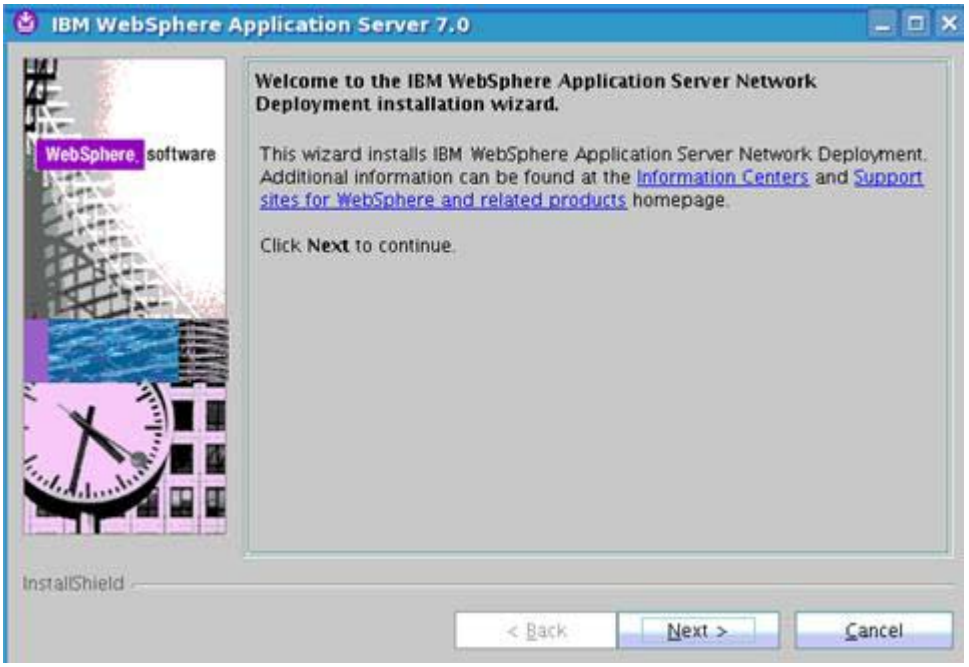


Figure 17. IBM WebSphere Application Server 7.0: Welcome

__ 16. Accept the license agreement and click **Next** to continue.

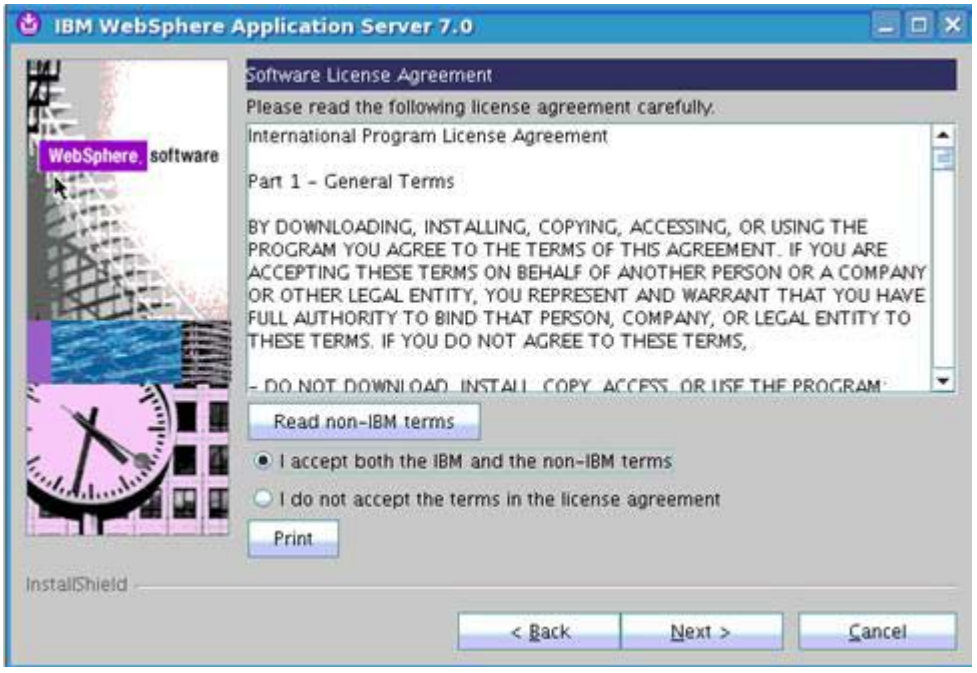


Figure 18. IBM WebSphere Application Server 7.0: Software License Agreement

__ 17. Click **Next** to continue.

Figure 19. IBM WebSphere Application Server 7.0: System Prerequisites Check

__ 18. Do not select any options in the following panel and click **Next** to continue.

Figure 20. IBM WebSphere Application Server 7.0: Optional Features Installation

__ 19. Use the default path (if possible) and click **Next** to continue.

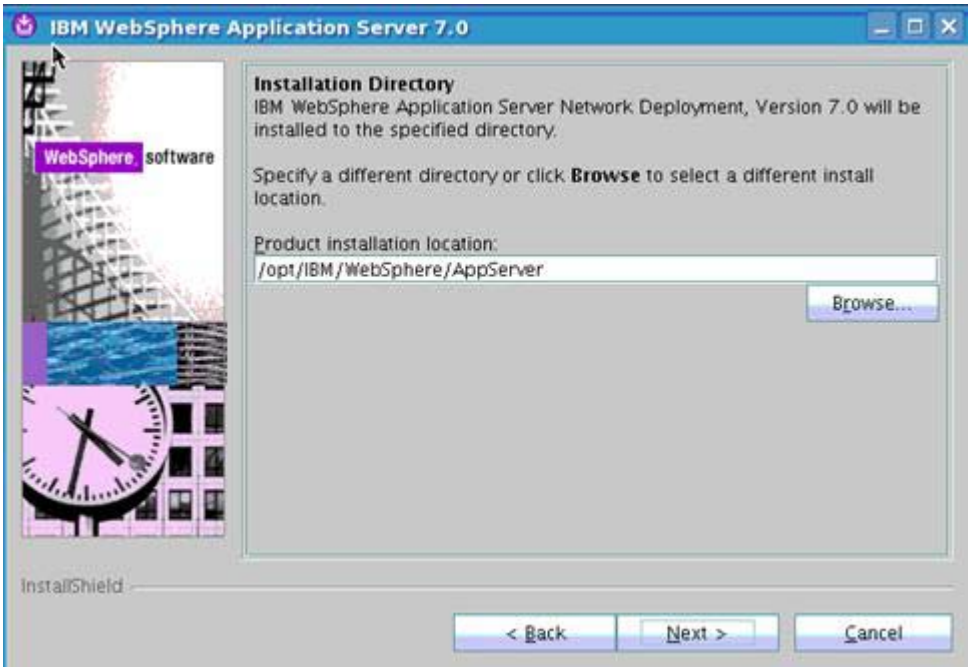


Figure 21. IBM WebSphere Application Server 7.0: Installation Directory

__ 20. Select **Application Server** and click **Next** to continue.

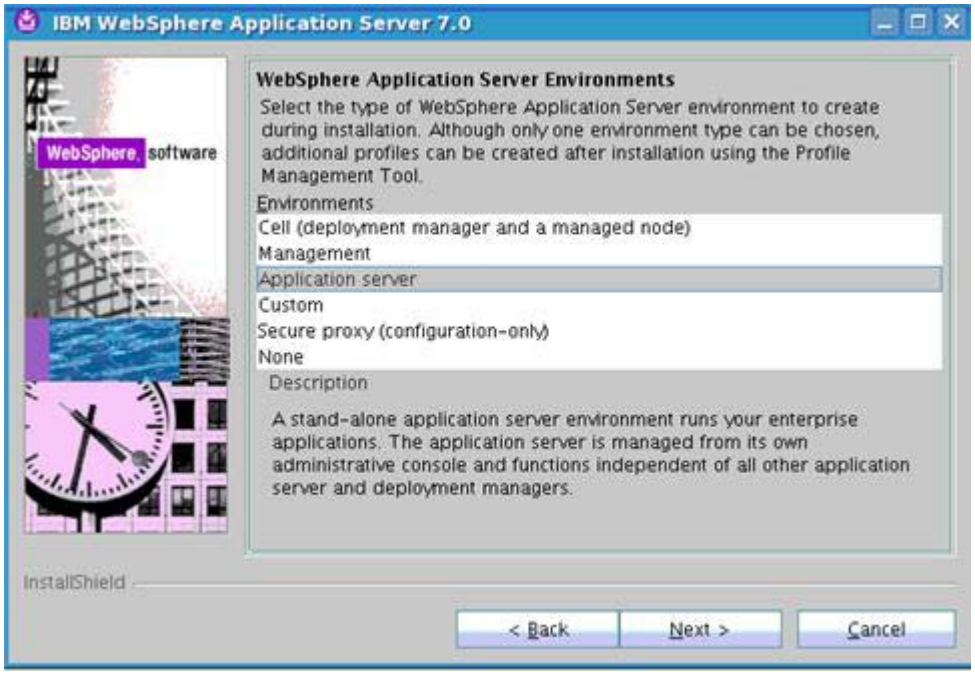


Figure 22. IBM WebSphere Application Server 7.0: WebSphere Application Server Environments

__ 21. Use the same user name and password that you used when you installed the Deployment Manager.

Figure 23. IBM WebSphere Application Server 7.0: Enable Administrative Security

__ 22. Click **Next** and verify the permissions.

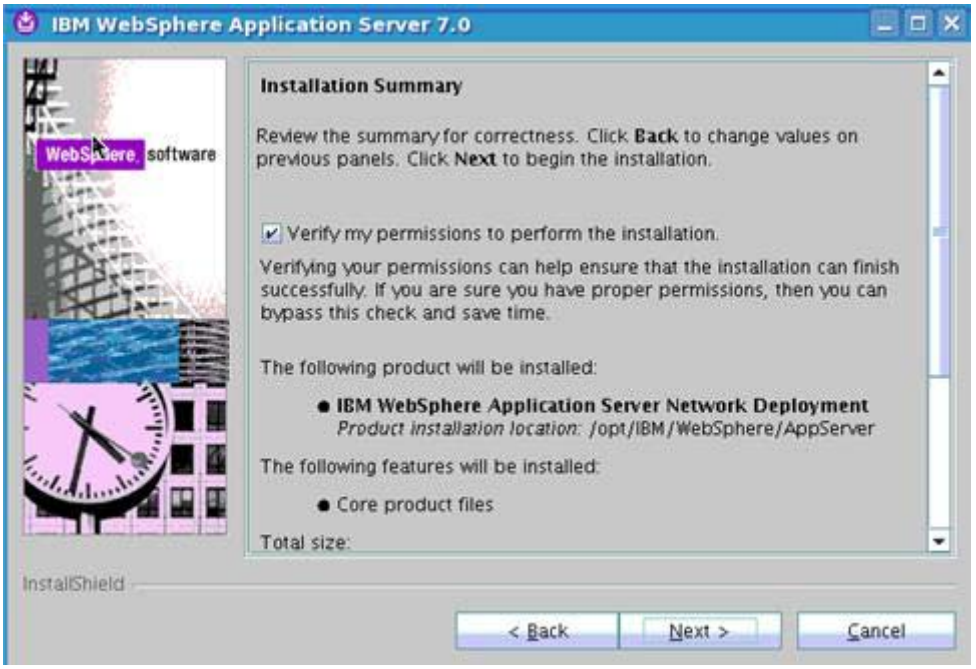


Figure 24. IBM WebSphere Application Server 7.0: Installation Summary: Verification

__ 23. When the verification finishes click **Next** to continue.

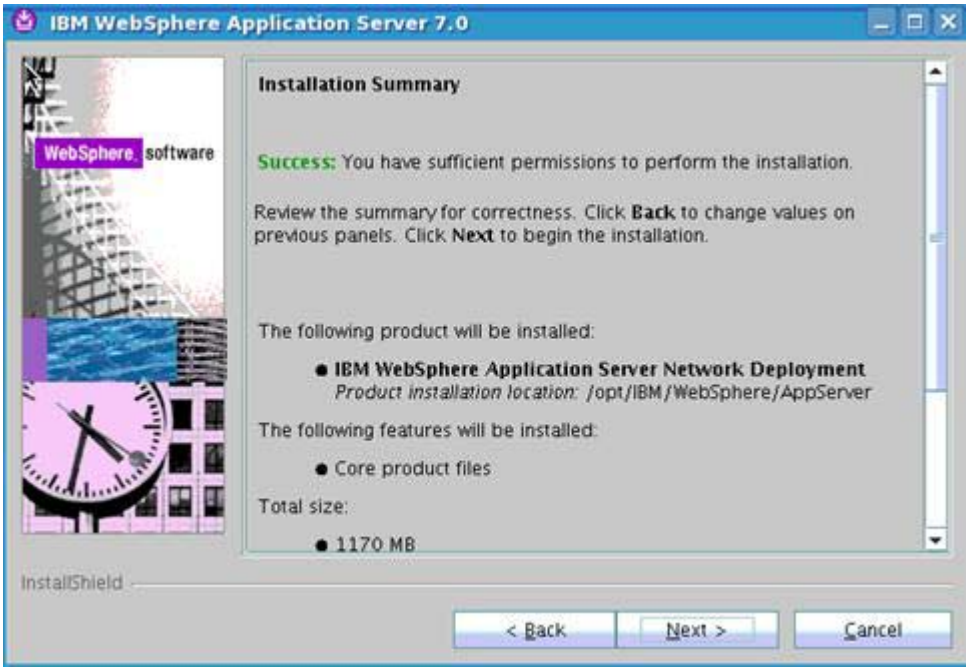


Figure 25. IBM WebSphere Application Server 7.0: Installation Summary

The installation starts to copy files.

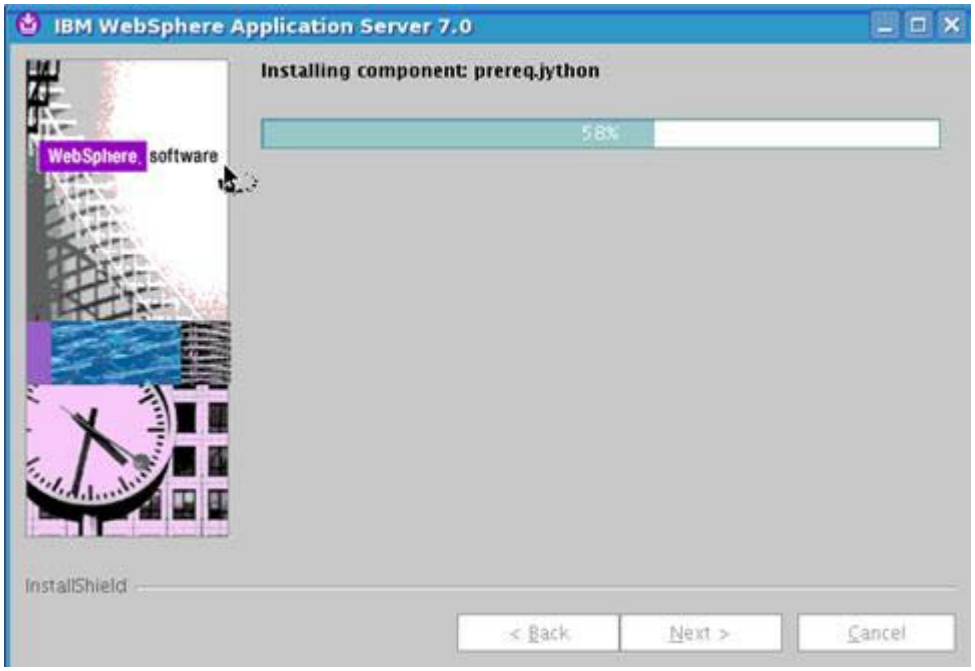


Figure 26. IBM WebSphere Application Server 7.0: Installation in progress

__ 24. After some time the installation finishes. Click **Finish** to exit the installer.

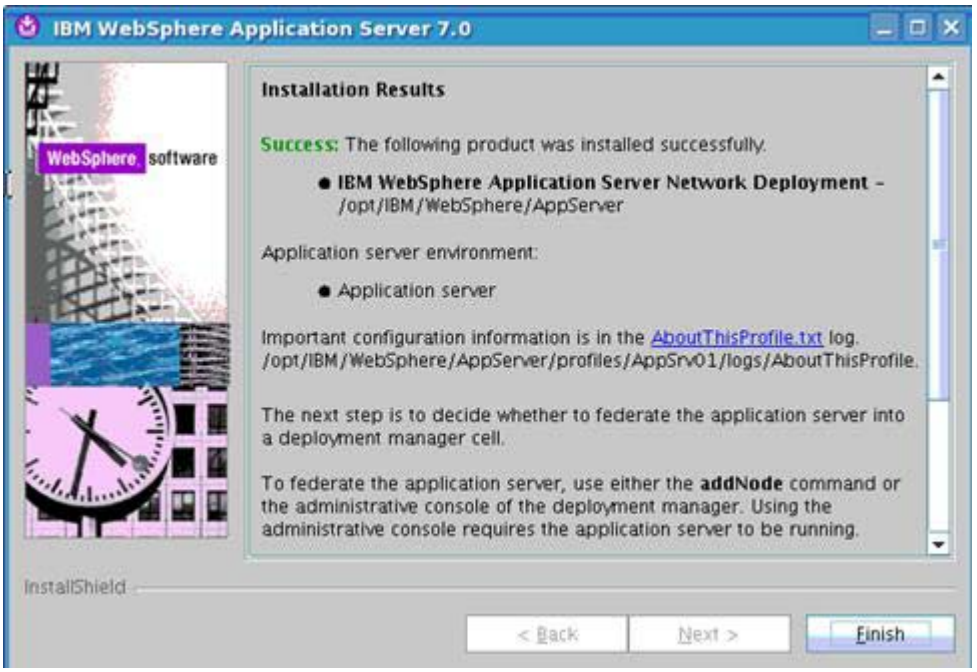


Figure 27. IBM WebSphere Application Server 7.0: Installation results

__ 25. Click **Installation verification**.

Figure 28. WebSphere Application Server: First steps: Installation verification

Here is the output.

Figure 29. First steps output: Installation verification

`Node1.spnego.company.com` is installed with WebSphere Application Server 7.0 AppServer.

__ 26. Now repeat these steps for `Node2.spnego.company.com` and the final screen should look like the following figure:

Figure 30. First steps output: Installation verification

Install/setup IBM HTTP Server (IBM HTTP Server) v7.0 and plug-ins

Note

Notes for the install/setup of IBM HTTP Server (IBM HTTP Server) v7.0 and plug-ins:

- The IBM HTTP Server is installed on `dm&ihs.spnego.company.com`.
- Check that all required OS libraries/packages are installed.

To complete this install, follow these steps:

__ 1. As `root`, go to the `../IBM HTTP Server` folder and start `install`.

__ 2. You see a screen like the following one. Click **Next**.

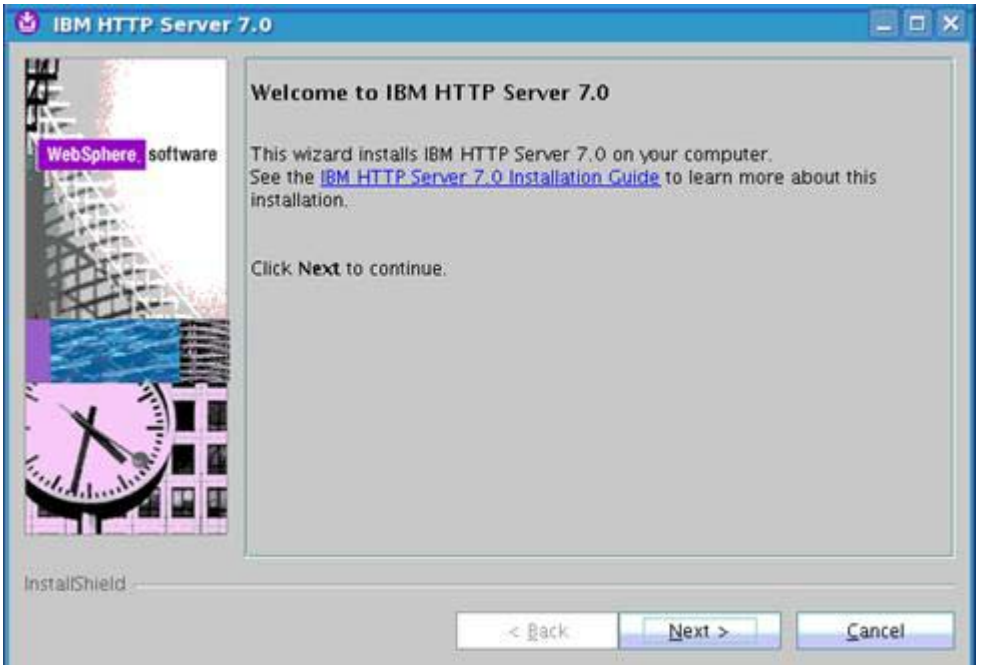


Figure 31. IBM HTTP Server 7.0: Welcome screen

__ 3. Accept the license agreement and click **Next**.

Figure 32. IBM HTTP Server 7.0: Software License Agreement

__ 4. In the System Prerequisites Check panel, click **Next**.

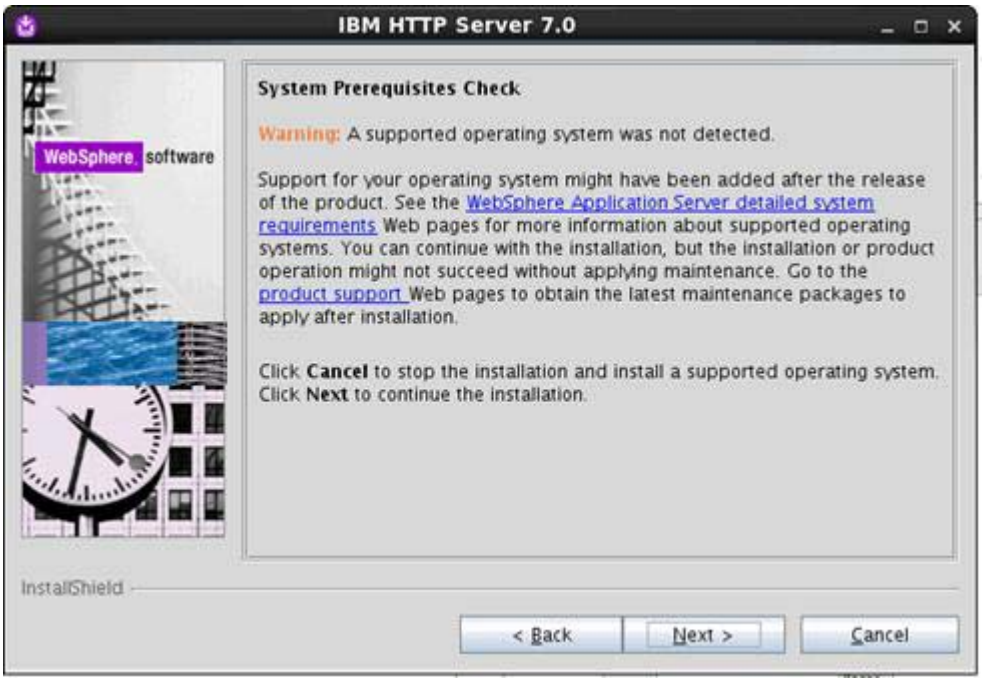


Figure 33. IBM HTTP Server 7.0: System Prerequisites Check

__ 5. Use the default installation location and then click **Next**.

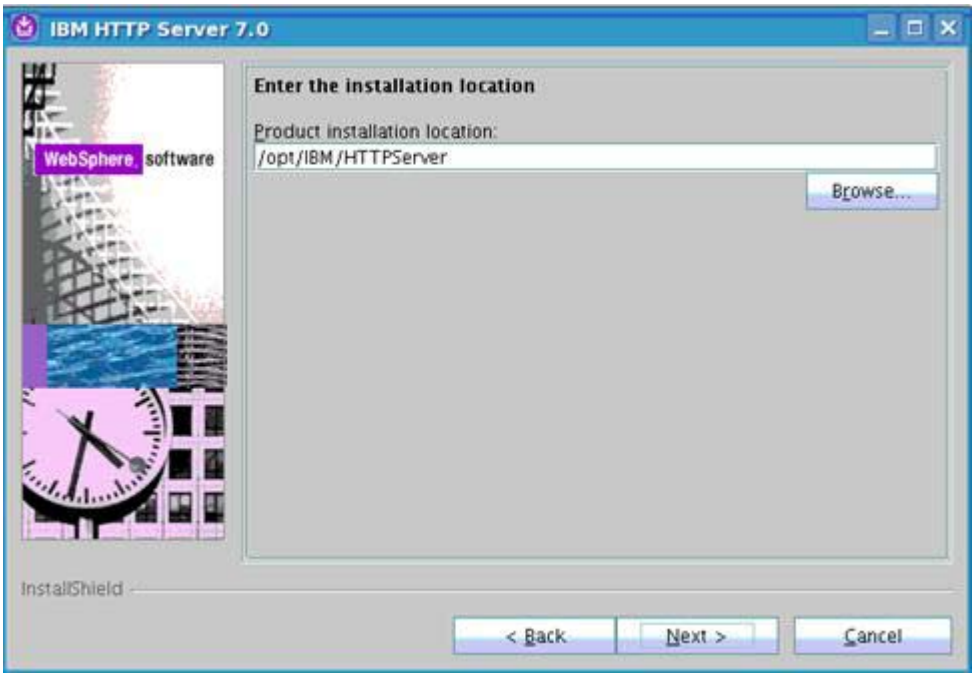


Figure 34. IBM HTTP Server 7.0: Enter the installation location

__ 6. Use default port and then click **Next**.

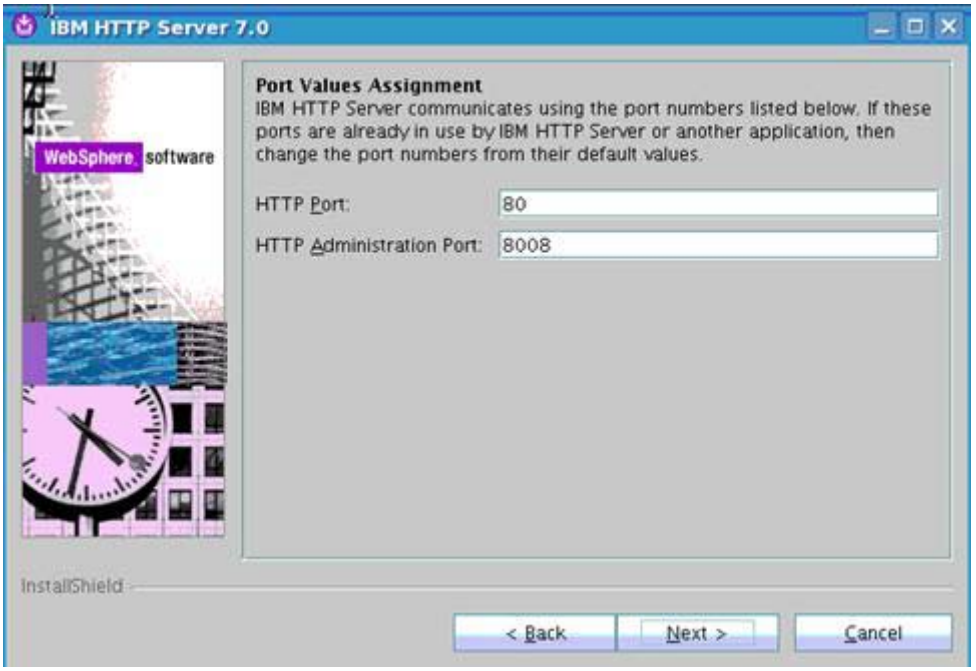


Figure 35. IBM HTTP Server 7.0: Port Values Assignment

__ 7. Specify the Admin ID (`ihsadmin`) and password and click **Next**.

Figure 36. IBM HTTP Server 7.0: HTTP Administration Server Authentication

__ 8. For the administration server use `ihsadmin` for the user ID and `ihsadmins` for the group.

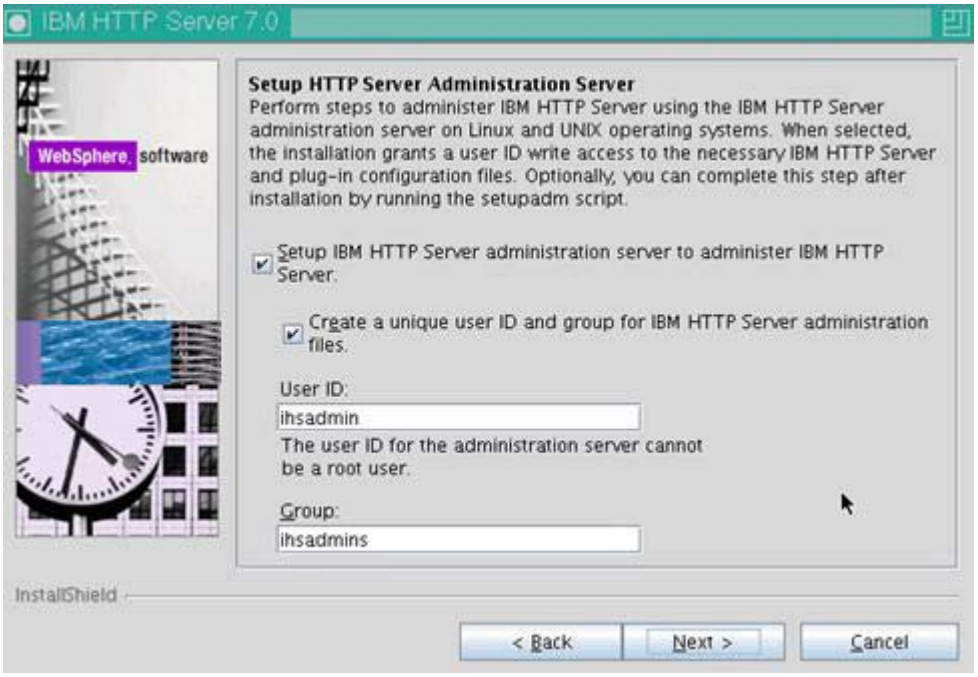


Figure 37. IBM HTTP Server 7.0: Setup HTTP Server Administration Server

__ 9. Enter `webserver1` for the web server definition and `dm&ihs.spnego.company.com` for the host name for the application server.

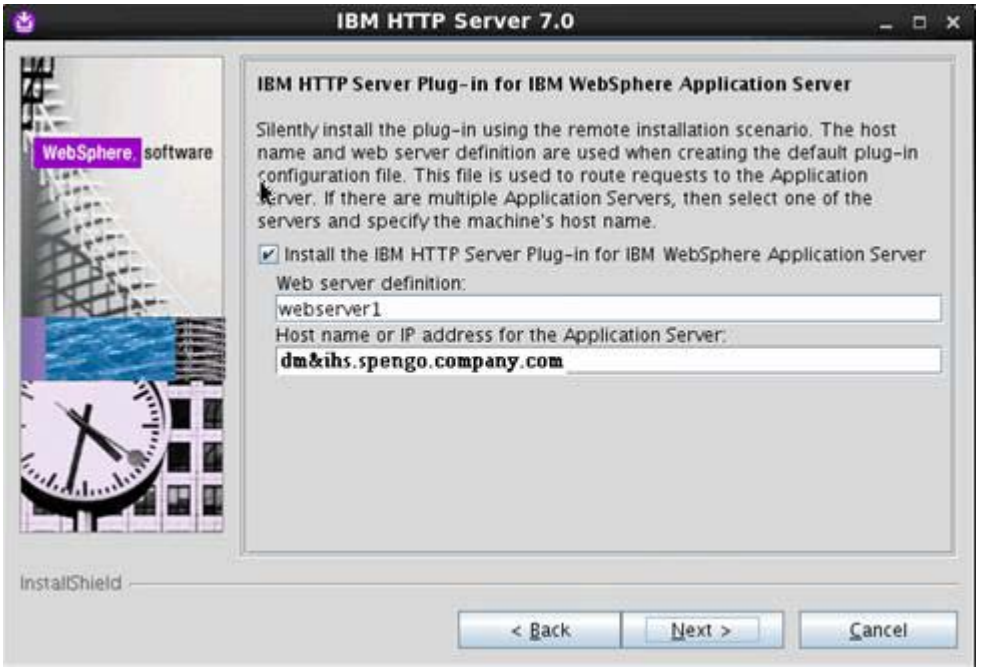


Figure 38. IBM HTTP Server 7.0: IBM HTTP Server plug-in for IBM WebSphere Application Server

__ 10. Review the summary information and click **Next** to start the installation.

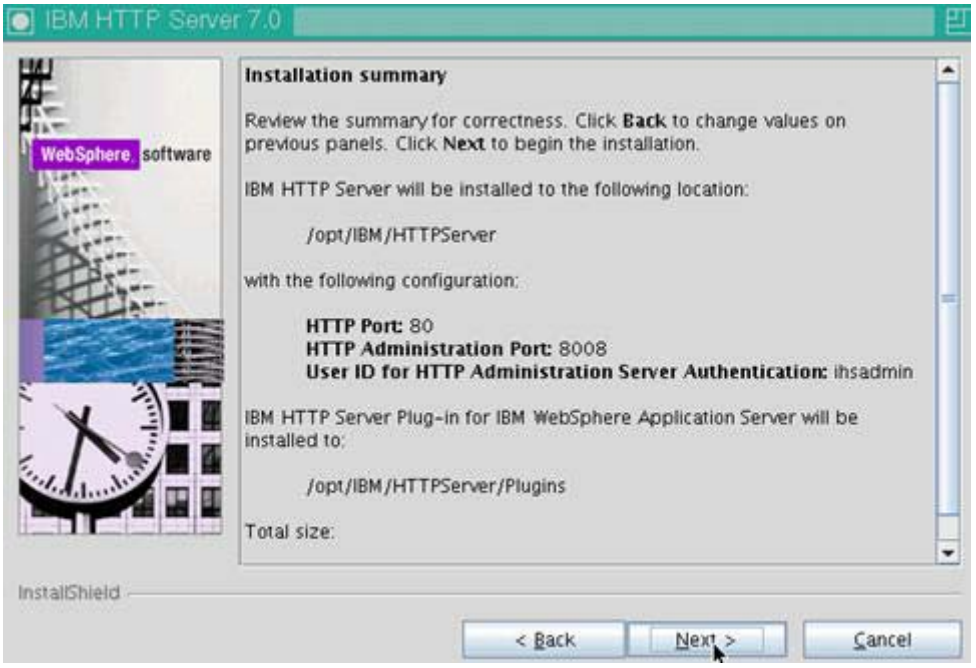


Figure 39. IBM HTTP Server 7.0: Installation summary

__ 11. After some time the installation completes. Then, click **Finish** to exit the wizard.

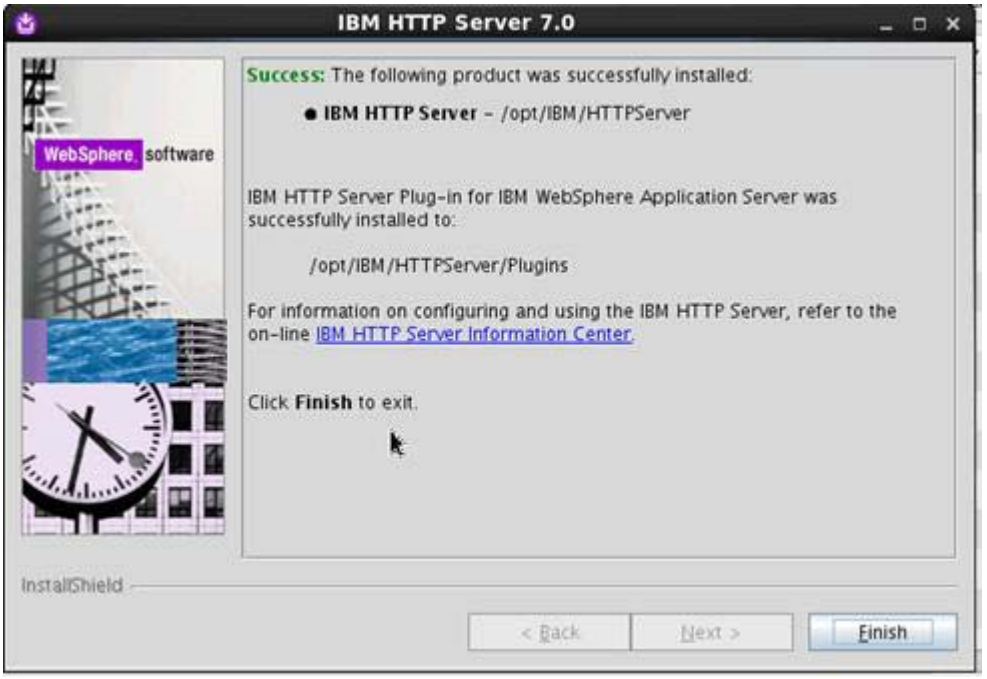


Figure 40. IBM HTTP Server 7.0: Installation successful

__ 12. Next, do the following steps:

__ a. Run the following command to create and set the IBM HTTP Server admin user and password:

```
/opt/IBM/HTTPServer/bin/htpasswd -cb
/opt/IBM/HTTPServer/conf/admin.passwd ihsadmin passw0rd
```

__ b. Verify that User and Group are set correctly in the `httpd.conf` file `vi httpd.conf` and verify that User and Group are set correctly as follows:

User `ihsadmin`

Group `ihsadmins`

__ c. Start apache server and the admin as follows:

```
/opt/IBM/HTTPServer/bin/apachectl start
/opt/IBM/HTTPServer/bin/adminctl start
```

__ d. Check the logs: `vi /opt/IBM/HTTPServer/logs/install/log.txt`.

__ 13. Verify that the IBM HTTP Server Webserver is running by entering the following address into your browser: `http://dm&ihs.spnego.company.com` and you should see the following screen:

Figure 41. WebSphere Software: IBM HTTP Server Version 7.0

Install WebSphere Application Server 7.0 Update Installer

__ 1. Download the WAS 7 Update Installer from Fix Central: `http://www-933.ibm.com/support/fixcentral/`.

__ 2. Copy the 7.0.0.21 Update Installer to your computer and uncompress the installation. Go to the folder `UpdateInstaller` and run `install`. You should see the panel below. Click **Next** to continue.

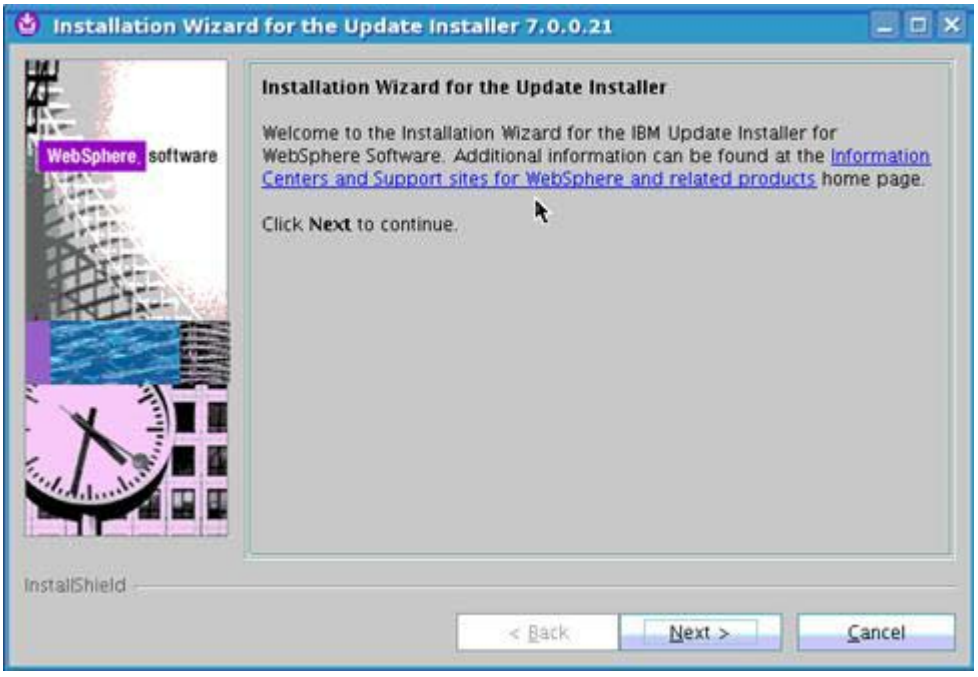


Figure 42. Installation Wizard for the Update Installer 7.0.0.9

__ 3. Accept the license agreement and click **Next** to continue.

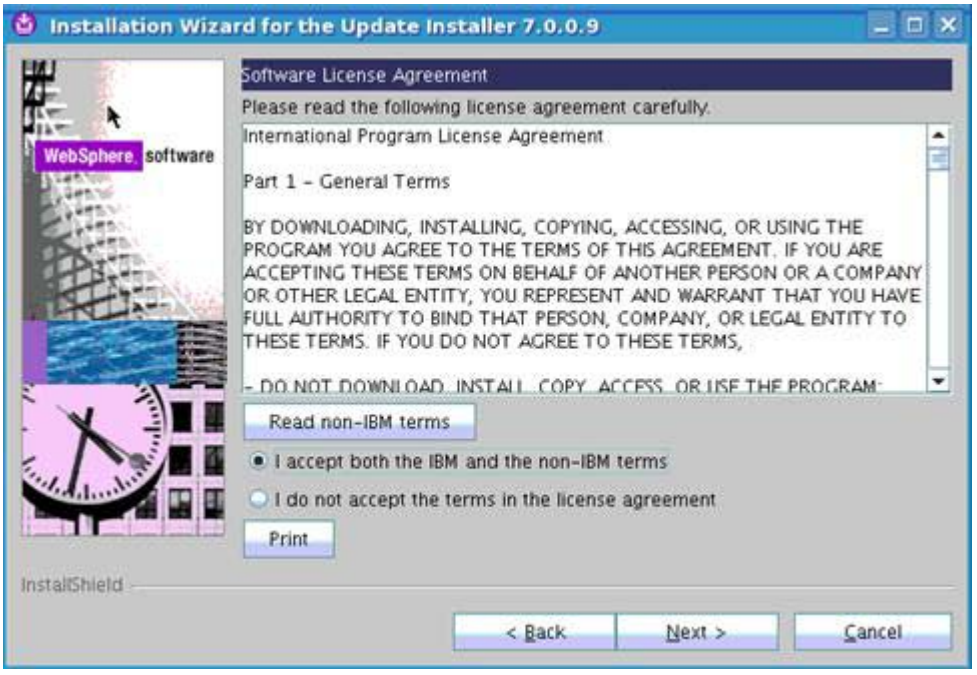


Figure 43. Installation Wizard for the Update Installer 7.0.0.9: Software license agreement

__ 4. In the System Prerequisites Check panel, click **Next**.

Figure 44. Installation Wizard for the Update Installer 7.0.0.9: System Prerequisites Check

__ 5. Use the default path if possible.

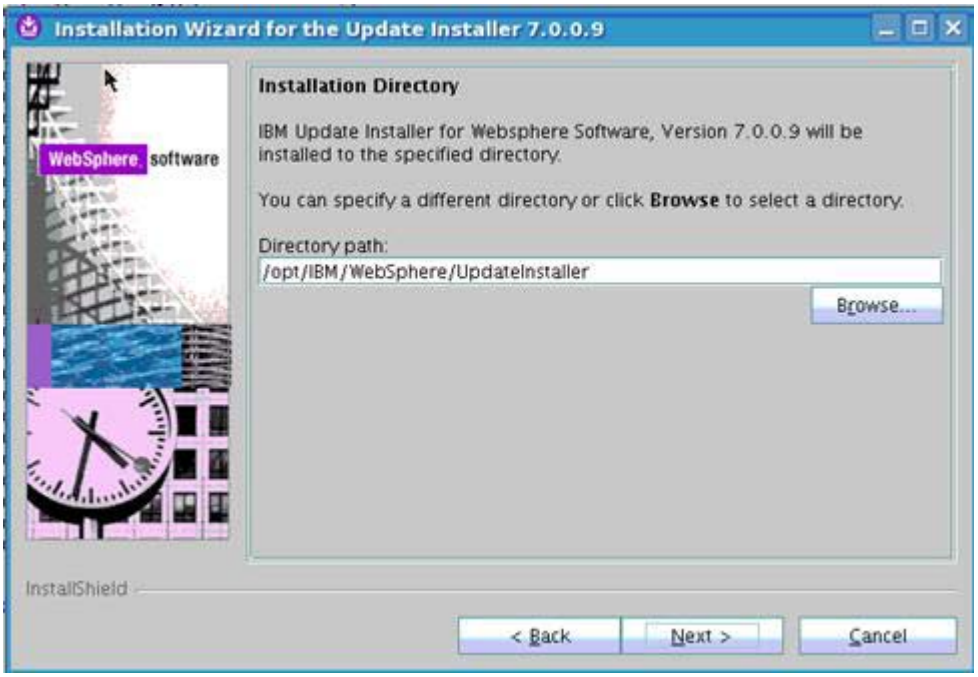


Figure 45. Installation Wizard for the Update Installer 7.0.0.9: Installation Directory

__ 6. In the summary screen, click **Next**.

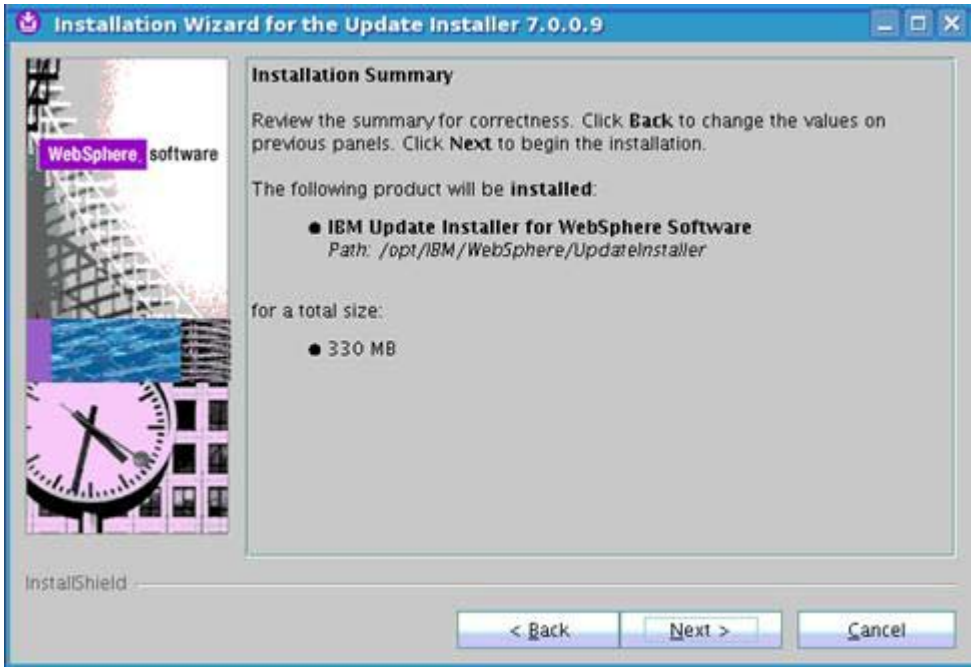


Figure 46. Installation Wizard for the Update Installer 7.0.0.9: Installation Summary

The installation of the files starts.

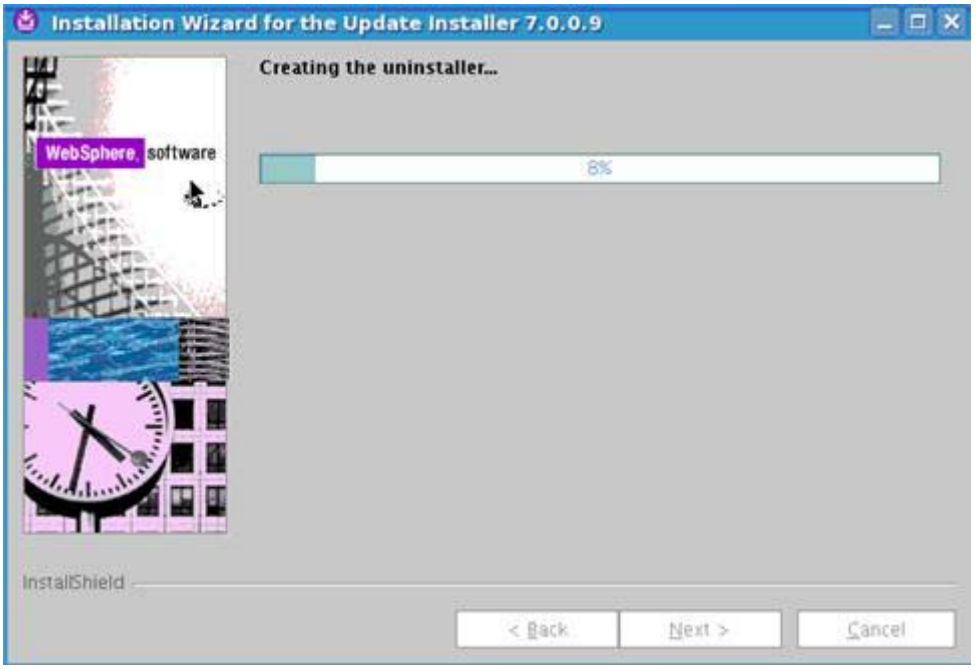


Figure 47. Installation Wizard for the Update Installer 7.0.0.9: Installation in progress

__ 7. After some time, it completes and you see the panel below. Click **Finish** to exit.

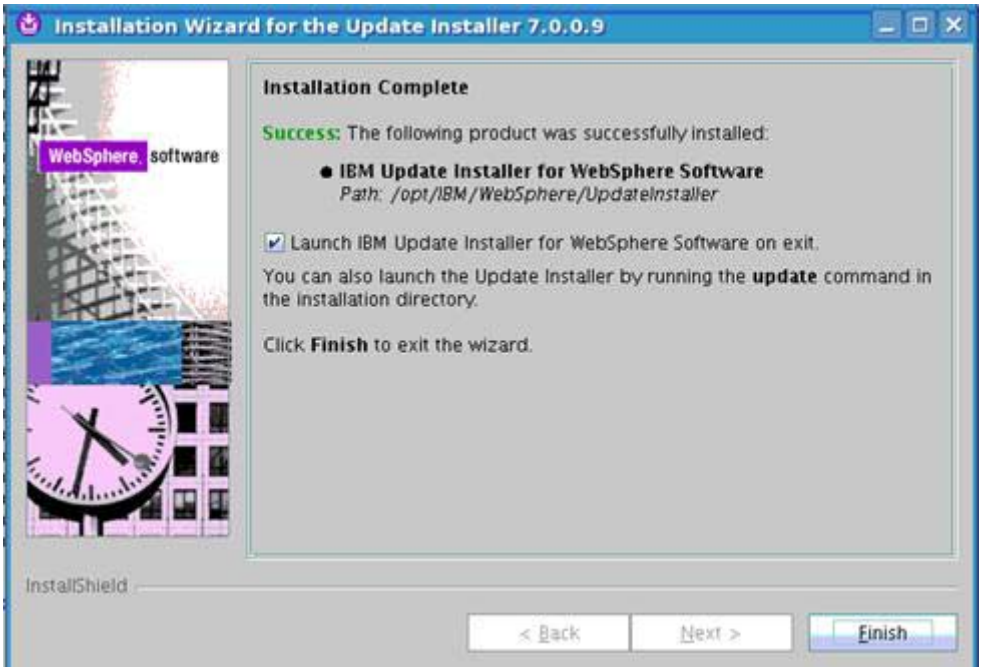


Figure 48. Installation Wizard for the Update Installer 7.0.0.9: Installation Complete

Now the WebSphere Application Server Update Installer is installed.

Update Deployment Manager, AppServer, IBM HTTP Server, IBM HTTP Server plug-ins, and SDKs to WebSphere Application Server 7.0 FixPack 21

__ 1. Download the `WebSphere Application Server 7.0 FP21` to the shared folder (on Deployment Manager and is accessible from node1 and node2). To install the WebSphere Application Server 7.0 FP21, do the following steps:

__ a. Stop your Deployment Manager, NodeAgents, AppServers, and IBM HTTP Server Server.

__ b. Start the WebSphere Application Server Update Installer by running `./update.sh` from under `/opt/IBM/WebSphere/UpdateInstaller/`. You should see the following screen.

__ c. Click **Next**.

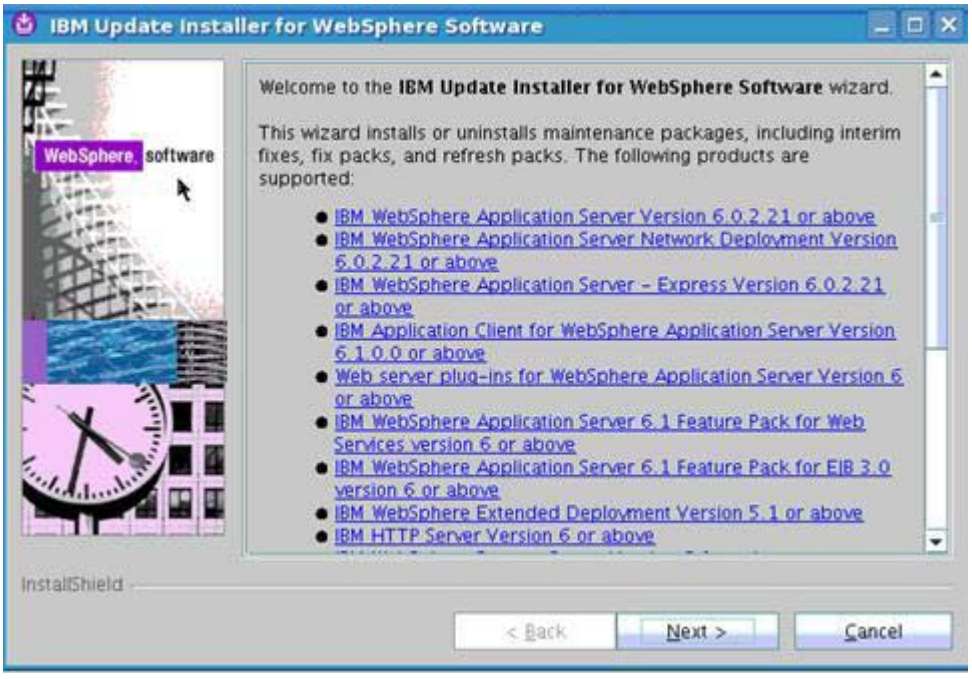


Figure 49. IBM Update Installer for WebSphere Software: Welcome

__ 2. Browse to the path of your Deployment Manager and click **Next**.

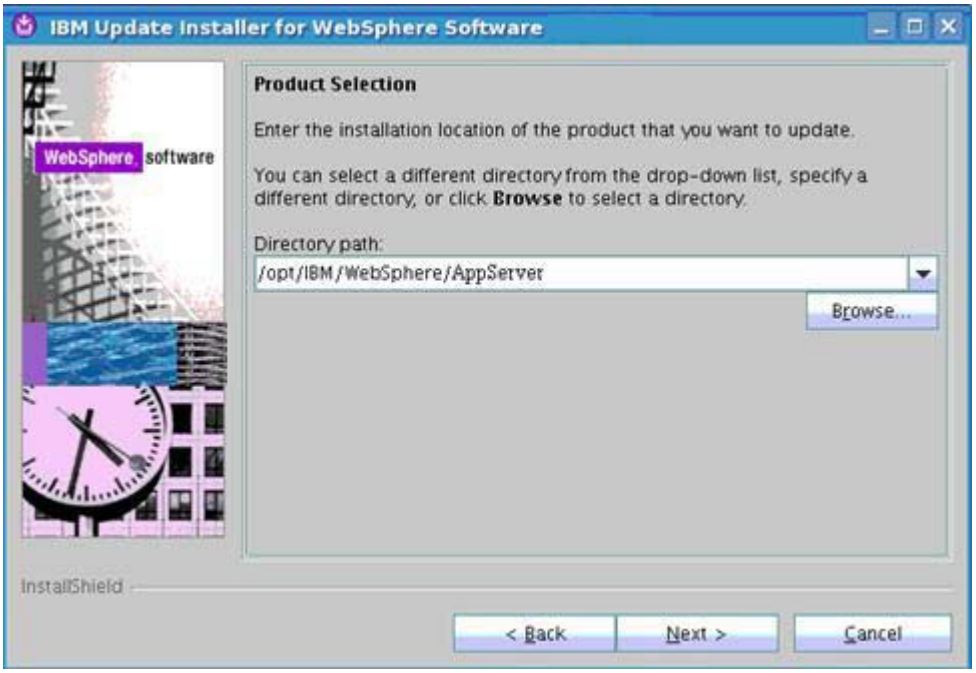


Figure 50. IBM Update Installer for WebSphere Software: Product Selection

__ 3. Select **Install maintenance package** and click **Next**.

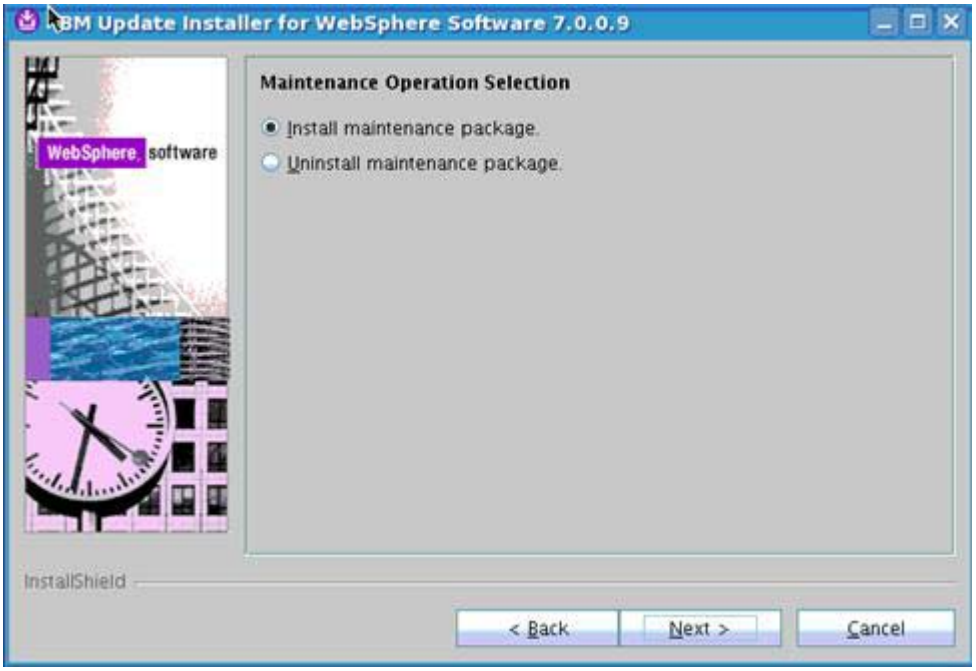


Figure 51. IBM Update Installer for WebSphere Software: Maintenance Operation Selection

__ 4. Browse to the path of your FP21 pak files. Click **Next**.

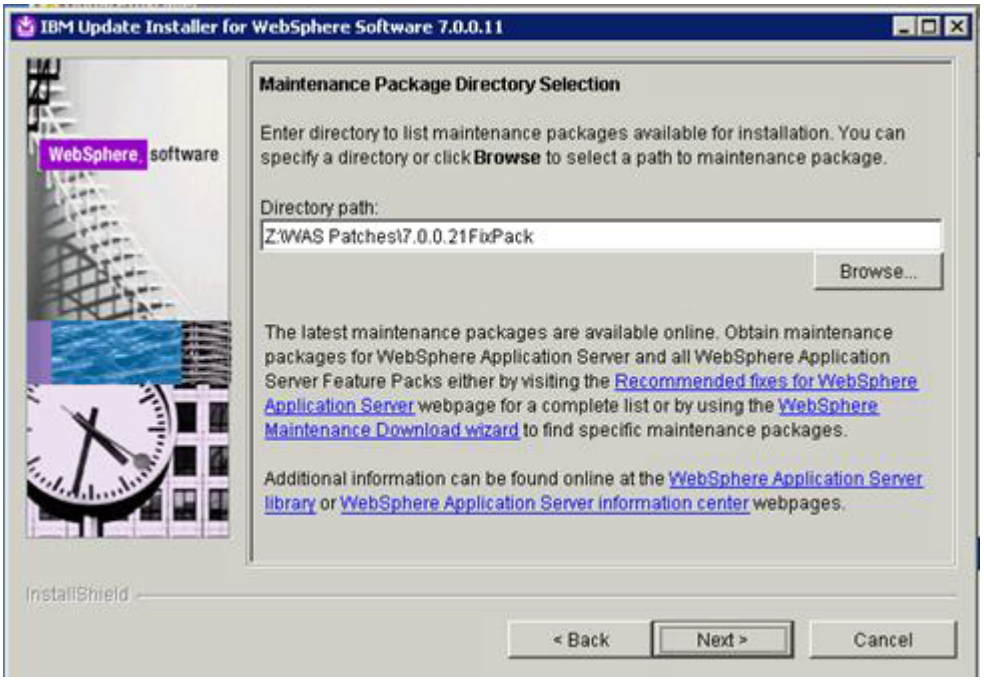


Figure 52. IBM Update Installer for WebSphere Software: Maintenance Package Directory Selection

__ 5. The installation picks up the two updates that need to be installed. Click **Next**.

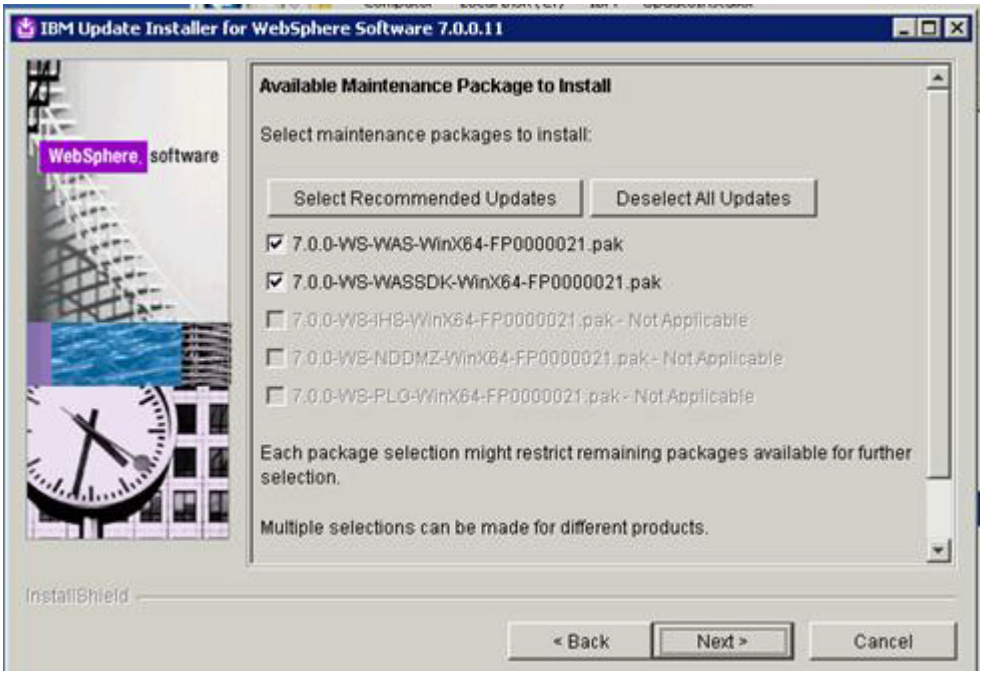


Figure 53. IBM Update Installer for WebSphere Software: Available Maintenance Package to Install

The installation begins.

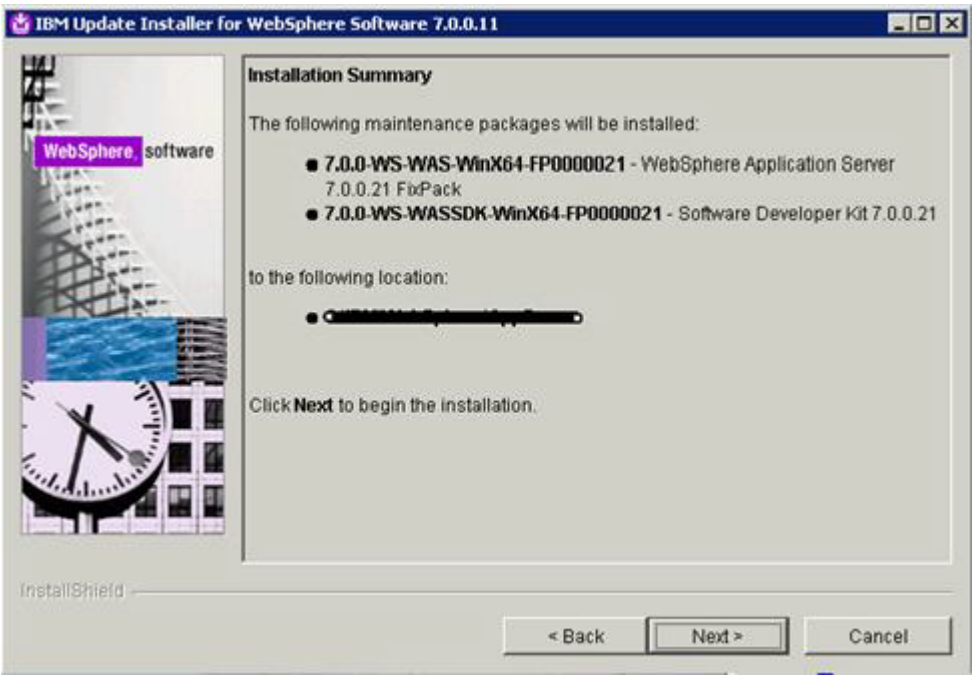


Figure 54. IBM Update Installer for WebSphere Software: Installation Summary

__ 6. After some time you see the following screen. Click **Relaunch**.

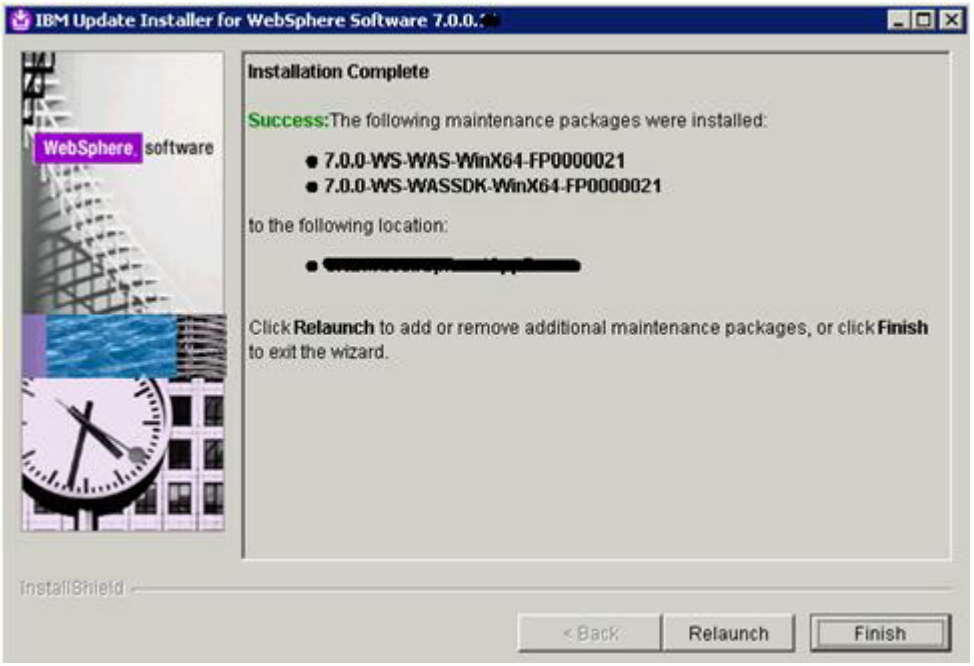


Figure 55. IBM Update Installer for WebSphere Software: Installation Complete

Note

'Relaunch' restarts the process. Then, repeat the steps for the following components:

- IBM HTTP Server
- IBM HTTP Server plug-in

__ 7. When it is completed, you should have all relevant WebSphere Application Server 7 FP21 updates installed on the following components:

   __ a. The Deployment Manager

   __ b. IBM HTTP Server

   __ c. IBM HTTP Server plug-in

__ 8. Next, install all relevant WebSphere Application Server 7 FP21 .pak files on each of the Nodes (that is, node1 and node2).

Federate WebSphere Application Server into the Deployment Manager

Next, you federate the AppServer into the deployment manager.

__ 1. Ensure that the clocks are in synch between your Deployment Manager and AppServer.

__ 2. Make sure that the Deployment Manager is started and the AppServers are stopped.

__ 3. Then, from both the Nodes (node1 & node2) within the folder `/opt/IBM/WebSphere/AppServer/bin` run the following command:

```
./addNode.sh dm&ihs.spnego.company.com 8879 -user wasadmin -password
wasadmin
```

You see:

```
ADMU0001I: Begin federation of node .        Node01 with Deployment Manager at
           [redacted] dm&ihs.spnego.company.com:8879.
ADMU0009I: Successfully connected to Deployment Manager Server:
           [redacted] dm&ihs.spnego.company.com:8879
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: server1
ADMU2010I: Stopping all server processes for node        .Node01
ADMU0512I: Server server1 cannot be reached. It appears to be stopped.
ADMU0024I: Deleting the old backup directory.
ADMU0015I: Backing up the original cell repository.
ADMU0012I: Creating Node Agent configuration for node:        .Node01
ADMU0014I: Adding node        Node01 configuration to cell:        Cell01
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: dslvm204Node01
ADMU0020I: Reading configuration for Node Agent process: nodeagent
ADMU0022I: Node Agent launched. Waiting for initialization status.
ADMU0030I: Node Agent initialization completed successfully. Process id is:
           7147


ADMU0300I: The node        Node01 was successfully added to the        Cell01
           cell.


ADMU0306I: Note:
ADMU0302I: Any cell-level documents from the standalone        Cell01
           configuration have not been migrated to the new cell.
ADMU0307I: You might want to:
ADMU0303I: Update the configuration on the        Cell01 Deployment Manager
           with values from the old cell-level documents.


ADMU0306I: Note:
ADMU0304I: Because -includeapps was not specified, applications installed on
           the standalone node were not installed on the new cell.
ADMU0307I: You might want to:
ADMU0305I: Install applications onto the        Cell01 cell using wsadmin
           $AdminApp or the Administrative Console.


ADMU0003I: Node        Node01 has been successfully federated.
```

Figure 56. Command ./addNode.sh dm&ihs.spnego.company.com 8879 -user wasadmin -password wasadmin

__ 4. When it is done:

__ a. Log in to your Deployment Manager at `http://dm&ihs.spnego.company.com:9060/admin`.

__ b. Go to **Servers > Server Types > WebSphere Application Servers**. You should see something like the following screen.

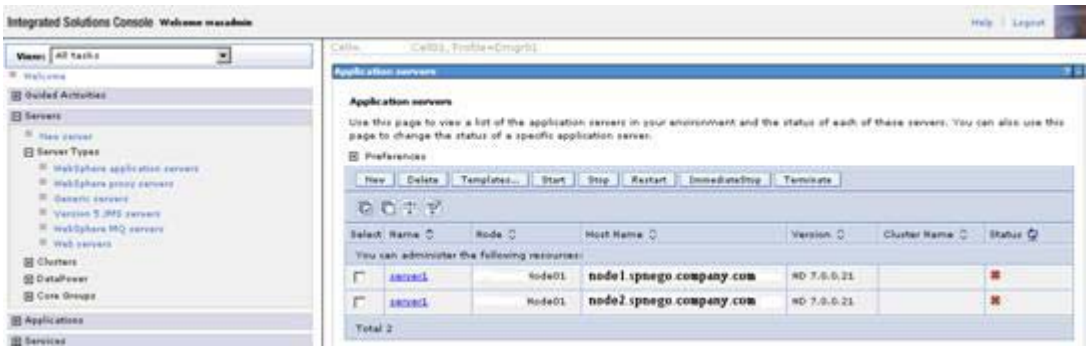


Figure 57. Application servers

Enable security on your Deployment Manager

Next, you add the LDAP repository to your Configuration.

General settings

__ 1. Start WebSphere Application Server and log in to your admin console `http://dm&ihs.spnego.company.com:9060/admin` (use wasadmin user and password).

__ 2. Select **Security > Global security**. Ensure that **Enable administrative security** and **Enable application security** are selected. Also, ensure that the **User account repository > Available realm definitions** is set to **Federated repositories**.

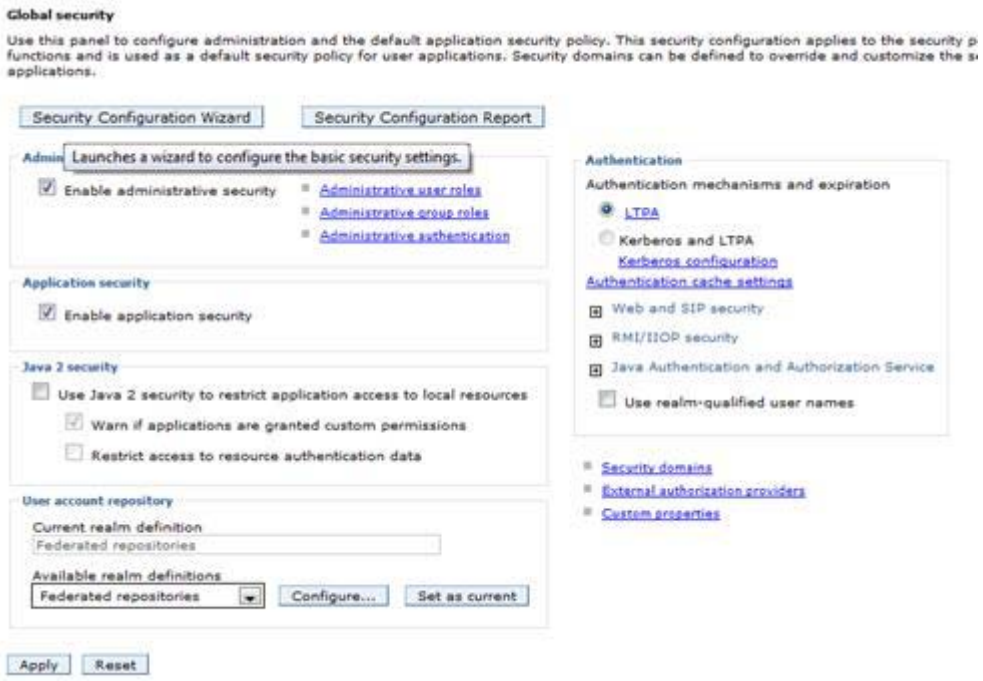


Figure 58. Global security

__ 3. Select **Apply** and save.

__ 4. Select **Security > Global security > Web and SIP Security > General Settings**.

__ 5. Ensure that **Use available authentication data when an unprotected URI is accessed** is selected.

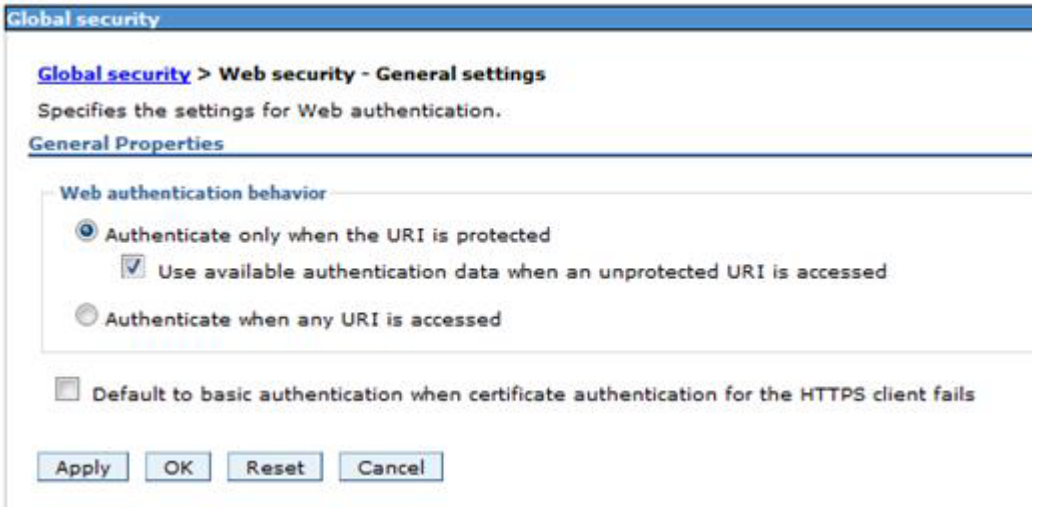


Figure 59. Web authentication behavior

__ 6. Click **Apply** and save.

__ 7. Select **Security > Global security > Web and SIP Security > Single sign-on (SSO)**.

__ 8. Ensure that **Interoperability Mode** is selected and enter the domain name `".spnego.company.com"`.

Important

Be sure to add the perior (.) before the domain name.

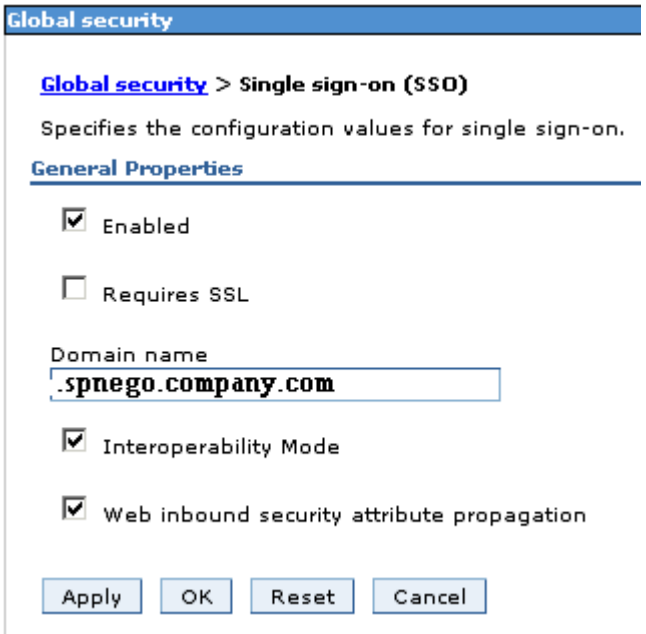


Figure 60. Global security: Domain name

__ 9. Select **Apply** and save.

Federate LDAP repositories

__ 1. Log in to your admin console `http://dm&ihs.spnego.company.com:9060/admin` (use wasadmin user and password).

__ 2. Select **Security > Global security > Configure**... for **Federated repositories**.

Figure 61. User account repository

__ 3. Select **Add Base entry to Realm**...

Figure 62. Repositories in the realm

__ 4. Then, select **Add Repository...**

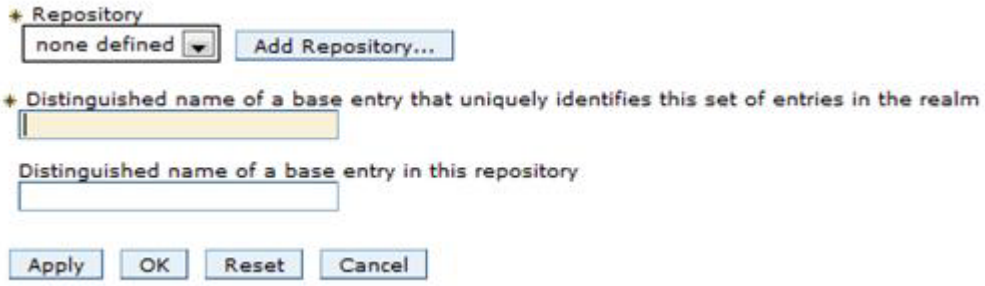


Figure 63. Adding repository

__ 5. Enter the following items:

__ a. Repository identifier

__ b. Primary host name

__ c. Bind distinguished name

__ d. Bind password

__ e. Login properties

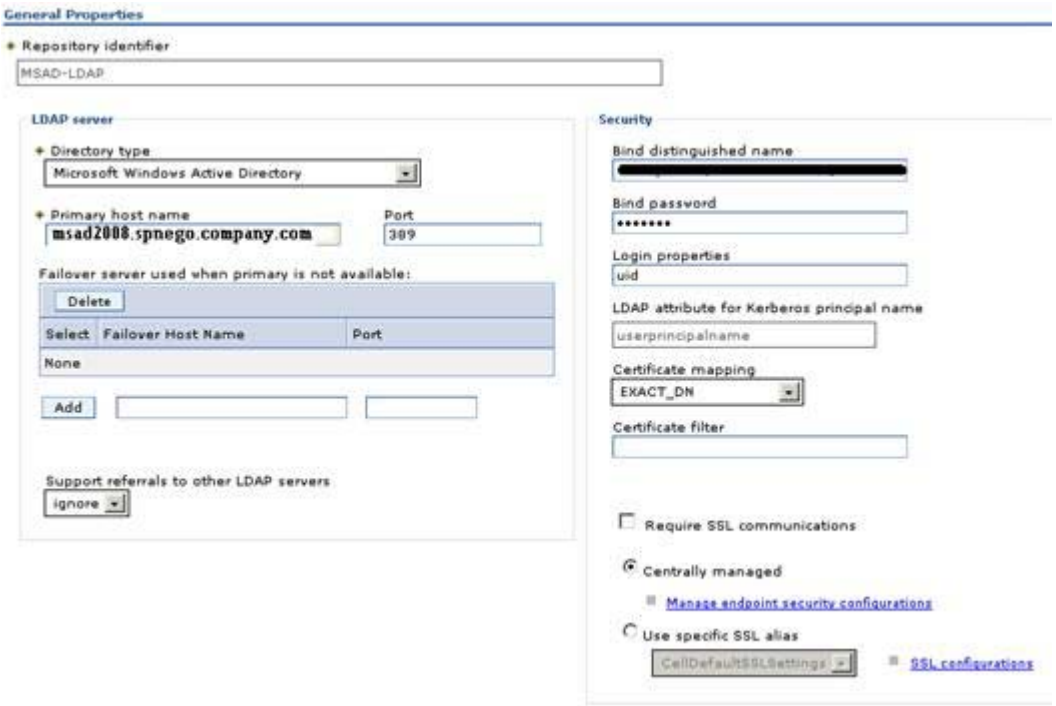


Figure 64. Repository identifier

__ 6. Click **OK**.

__ 7. Then, you enter the base entry.

Figure 65. Entering the base entry

__ 8. Select **Apply** and save.

__ 9. Restart your Deployment Manager and Node Agents.

Add AdminFromLDAP user as a WebSphere Application Server Deployment Manager administrator

__ 1. Log in to your admin console `http://dm&ihs.spnego.company.com:9060/admin`.

__ 2. Click **Users and Groups > Administrative user roles**.

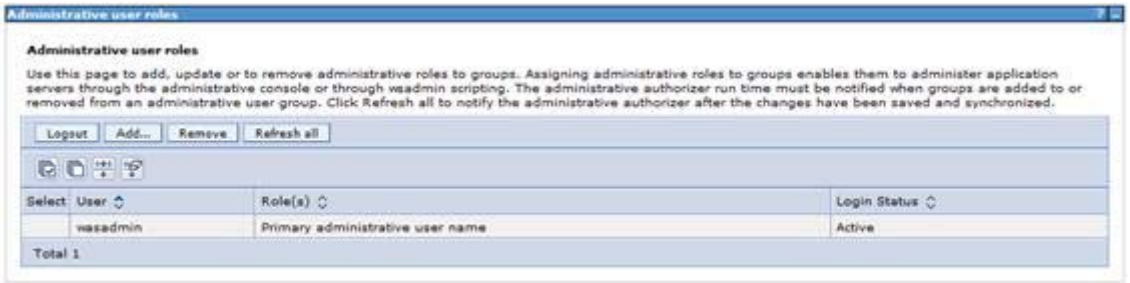


Figure 66. Administration user roles

__ 3. Click **Add**. Then, select the role `Administrator`, search for `AdminFromLDAP` and add that user to the M apped to Role.

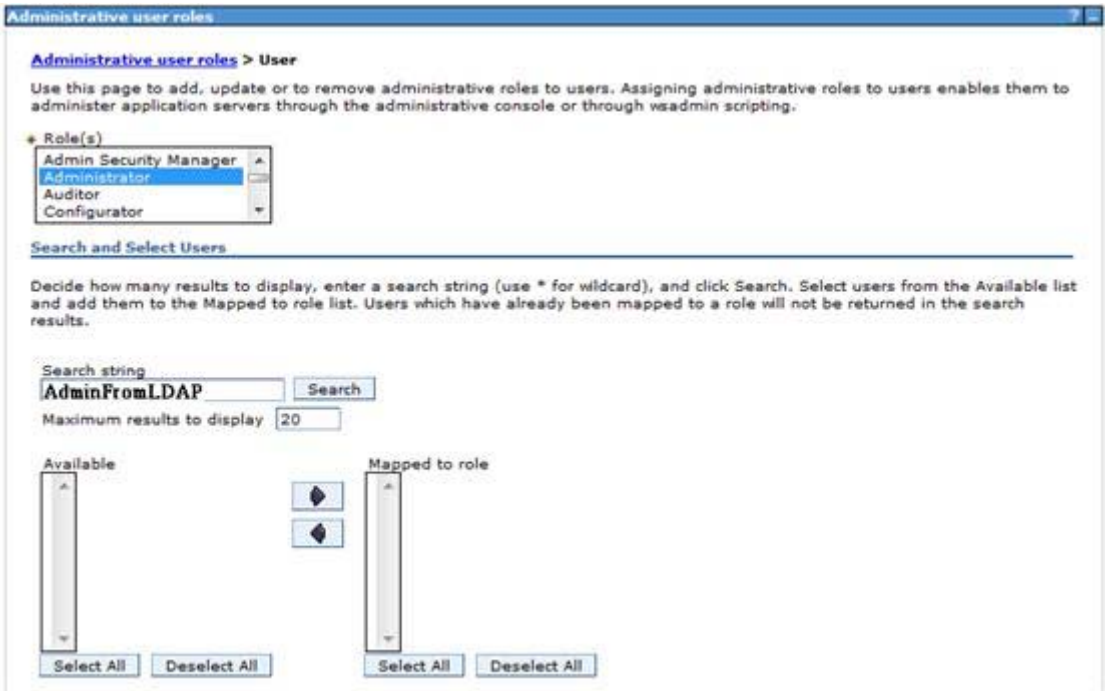


Figure 67. Search and Select Users

__ 4. Click **OK**.

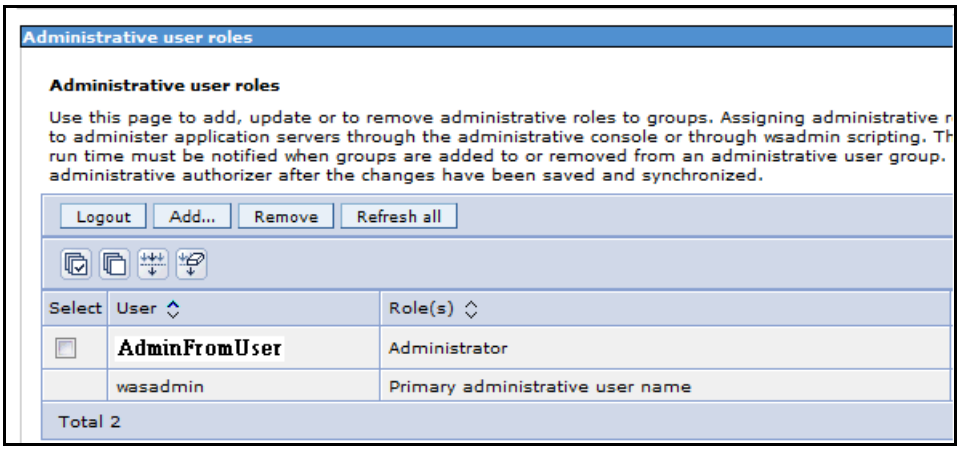


Figure 68. Administrative user roles

__ 5. Log out and then log back in again as AdminFromLDAP to ensure that it is working.

__ 6. Check that the nodes are in synch:

__ a. When logged in WebSphere Application Server Console as AdminFromLDAP, click **System Administration > Nodes**.

__ b. Check whether the nodes are in synch. The following figure shows the nodes in sync.

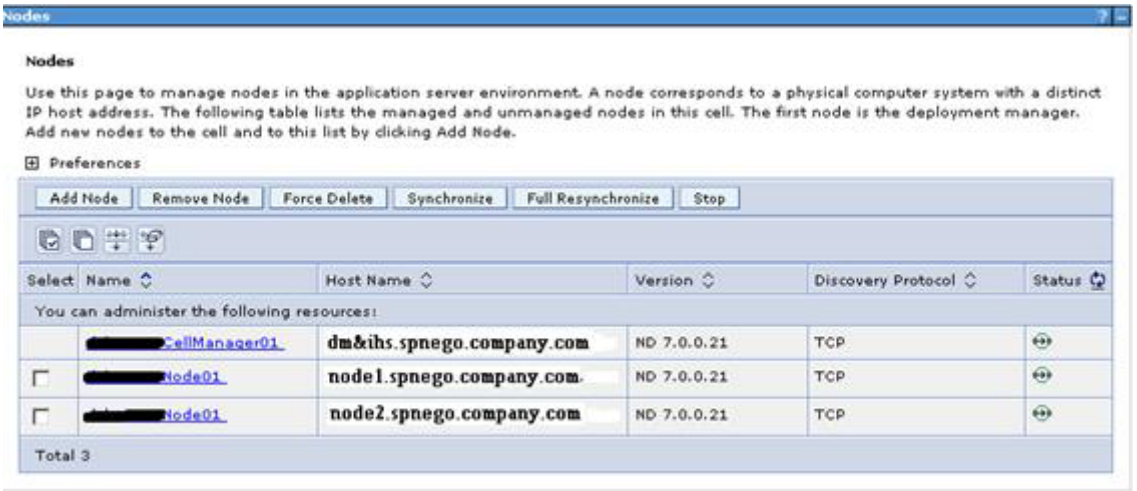


Figure 69. Nodes in synch

__ 7. If the nodes are not synchronizing as in the previous screen, then you can force Node synch from Node1 and Node2. Do the following on each node:

__ a. Stop the Node agents `./stopNode.sh`.

__ b. Run `./syncNode.sh dm&ihs.spnego.company.com 8878 -username UserFromLDAP -password password`.

__ c. Restart the node agents `./startNode.sh`.

__ d. Now recheck **System Administration > Nodes**. The nodes should now be in synch.

Installation of DB2 (V9.7-fp6) server

Note

DB2 9.7 FixPack 6 has the full DB2 installation.

__ 1. Copy the DB2 installation file DB2_ESE_V97-Fixpack6_Linux_x86-64.tar to your computer. Uncompress it and start the installer by running ./db2setup as the root user. You should see the following.

Figure 70. DB2 Setup Launchpad: Welcome

__ 2. Click **Install a Product** and then click **Install New** from the DB2 Enterprise Server Edition Version 9.7.

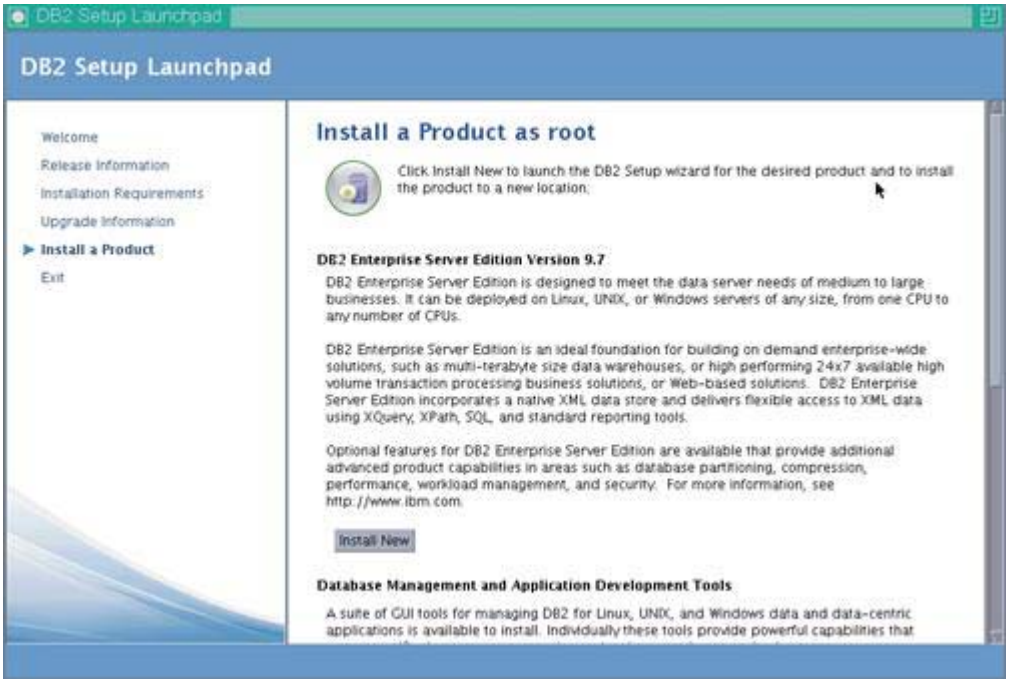


Figure 71. DB2 Setup Launchpad: Install a product as root

The DB2 installation wizard displays. Click **Next** to continue.

Figure 72. DB2 Setup wizard: Welcome

__ 3. Accept the license agreement and click **Next** to continue.

Figure 73. DB2 Setup wizard: Software License Agreement

__ 4. Click **Typical** as the installation type and then **Next** to continue.

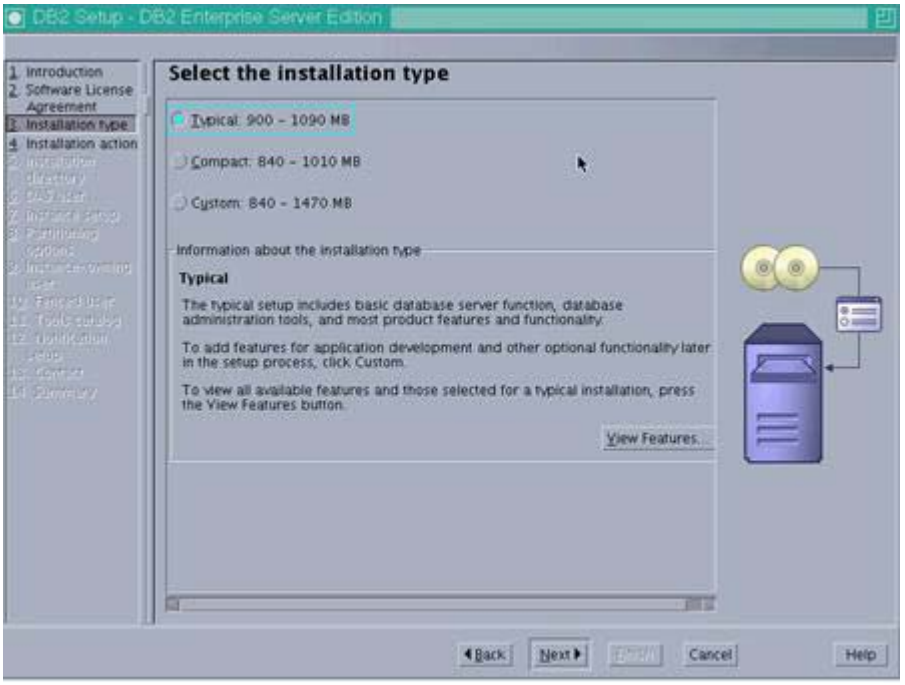


Figure 74. DB2 Setup wizard: Select the installation type

__ 5. Select the option “Install DB2 Enterprise Server Edition Version on this computer” and click **Next**.

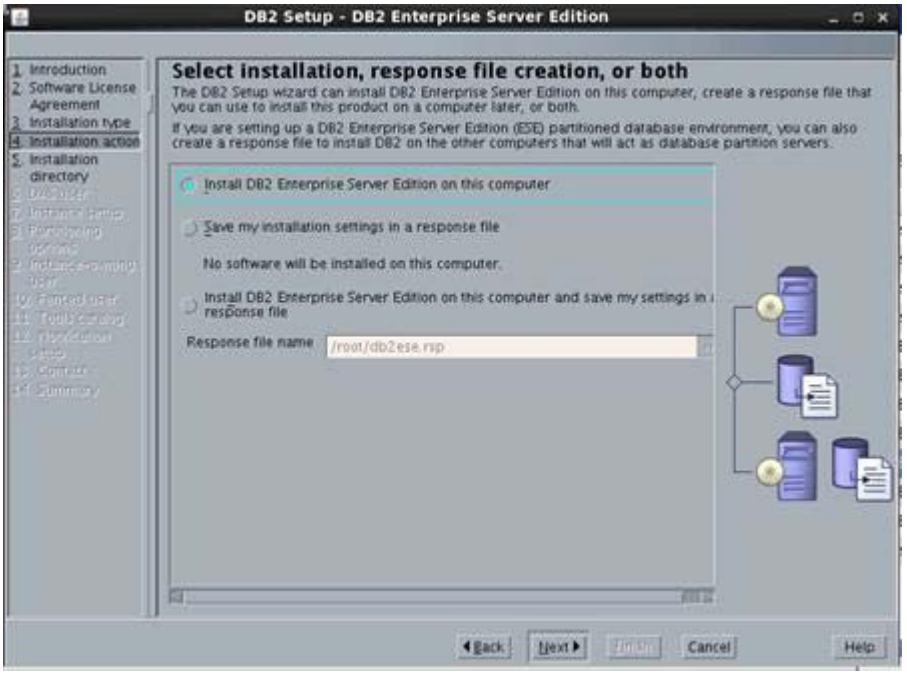


Figure 75. DB2 Setup wizard: Select installation, response file creation, or both

__ 6. Change the default path if you want. Then, click **Next** to continue.

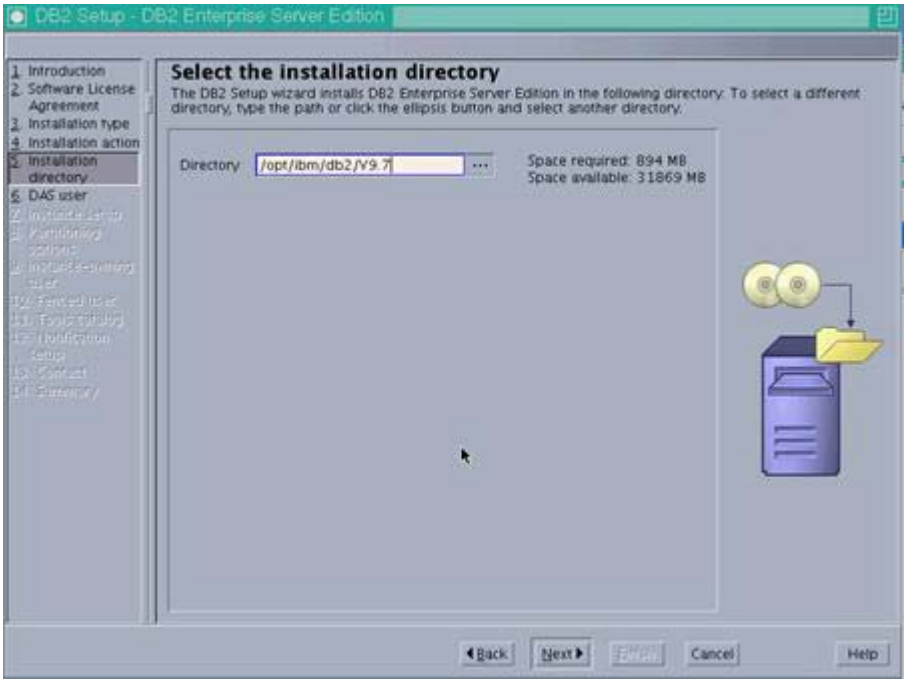


Figure 76. DB2 Setup wizard: Select the installation directory

__ 7. Enter the user name and password for the dasusr1 user and click **Next** to continue.

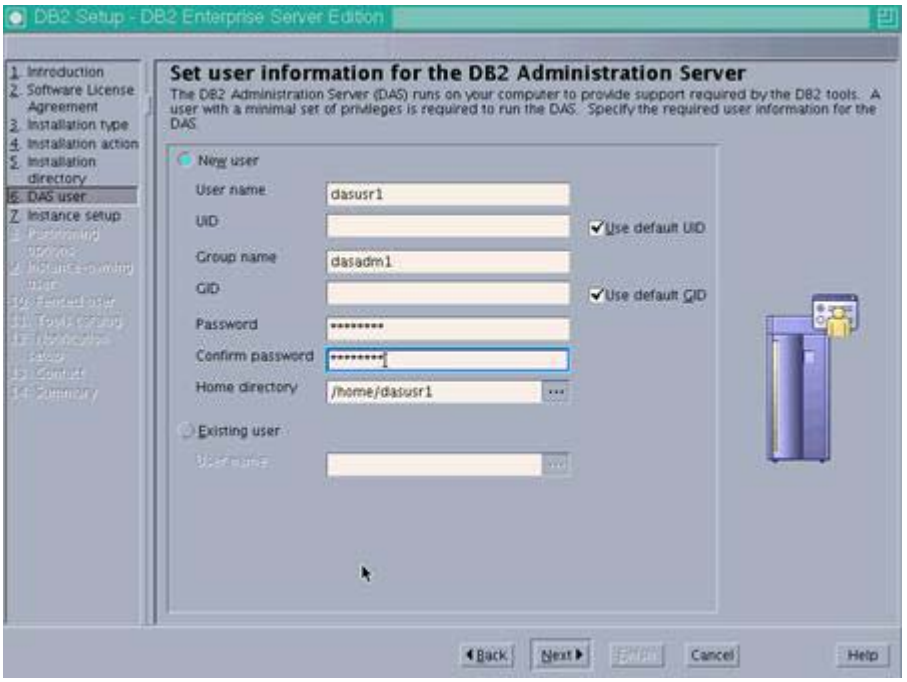


Figure 77. DB2 Setup wizard: Set user information for the DB2 Administration Server

__ 8. Select **Create a DB2 Instance**. Click **Next** to continue.

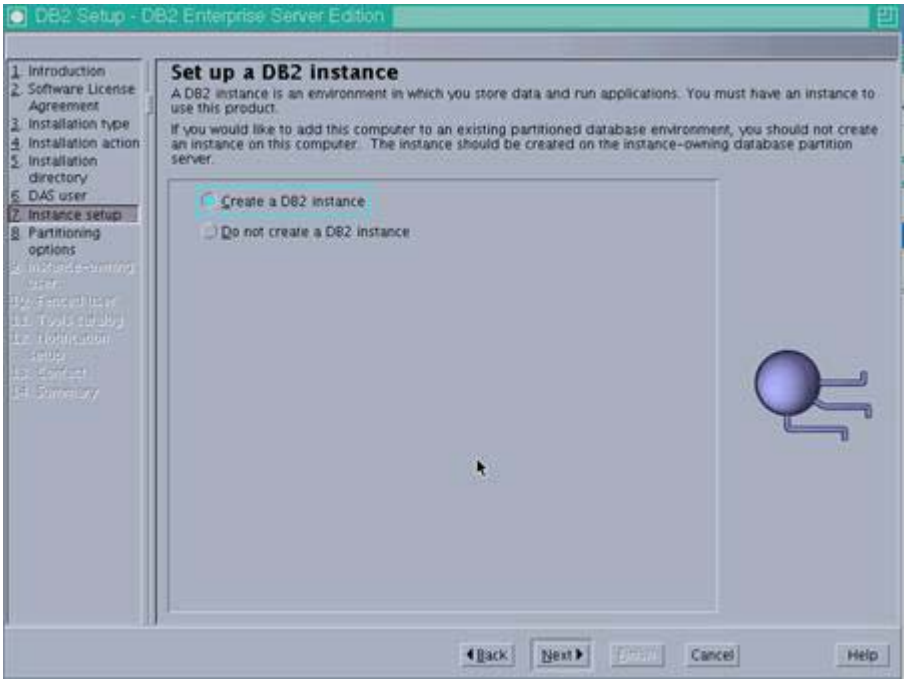


Figure 78. DB2 Setup wizard: Set up a DB2 instance

__ 9. Select **Single partition instance**. Click **Next** to continue.

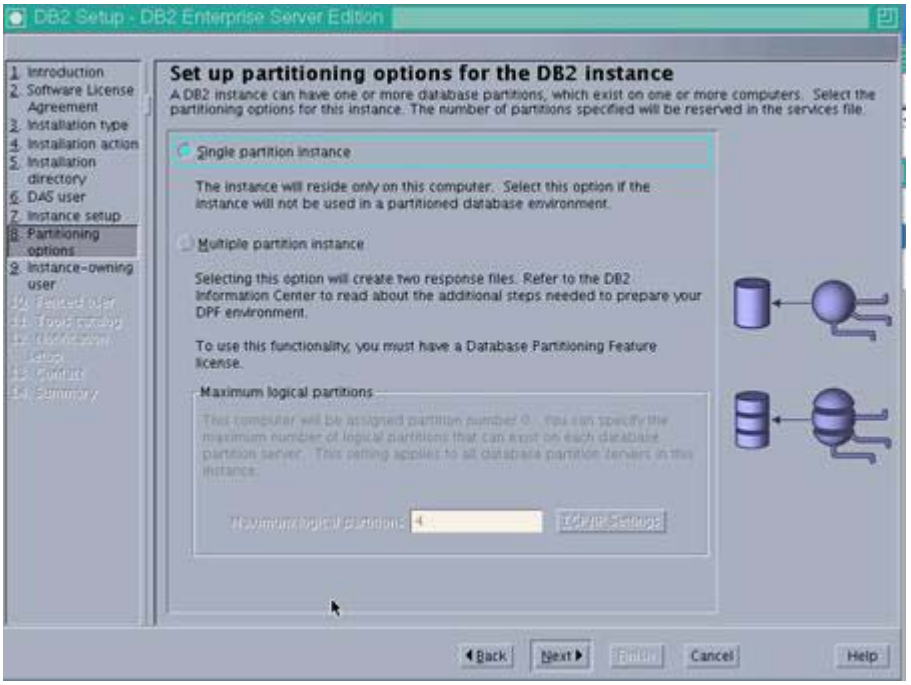


Figure 79. DB2 Setup wizard: Set up partitioning options for the DB2 instance

__ 10. Enter your database administrator user name and password. Then, click **Next** to continue.

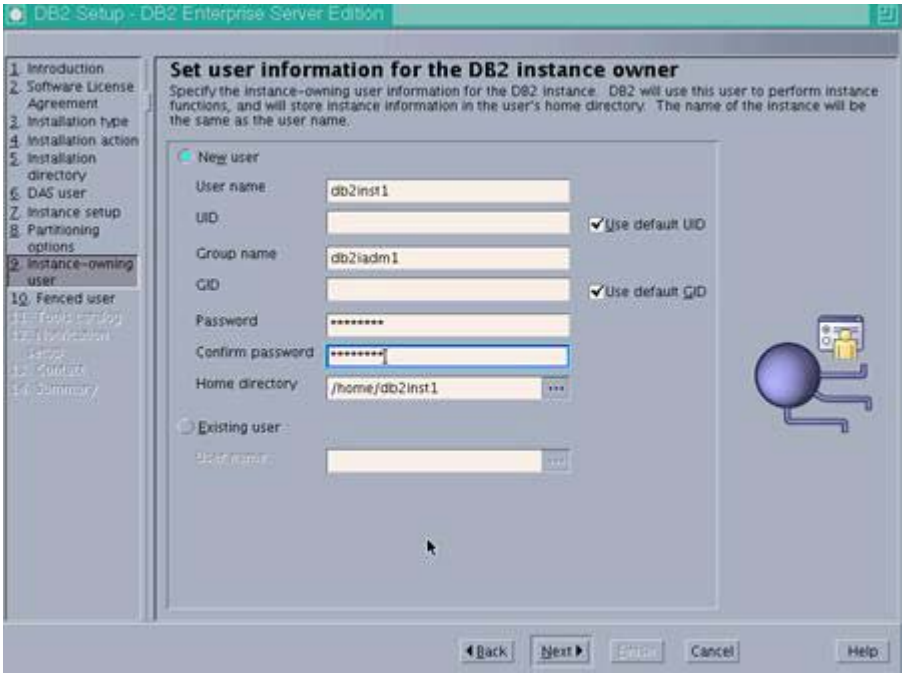


Figure 80. DB2 Setup wizard: Set user information for the DB2 instance owner

__ 11. Enter your fenced user name and password. Then, click **Next** to continue.

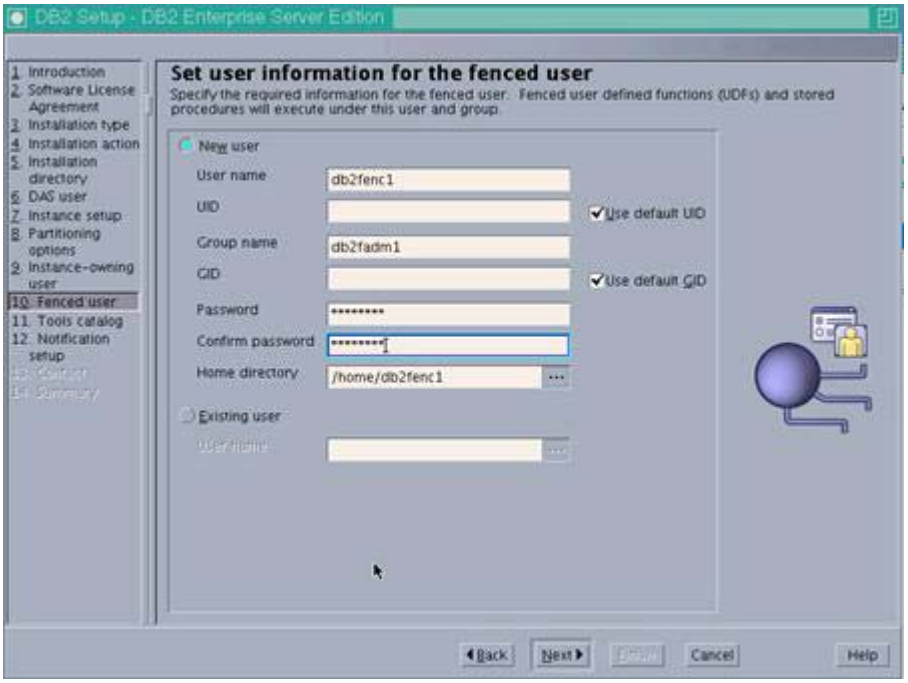


Figure 81. DB2 Setup wizard: Set user information for the fenced owner

__ 12. Select **Do not prepare the DB2 tools catalog** and click **Next** to continue.

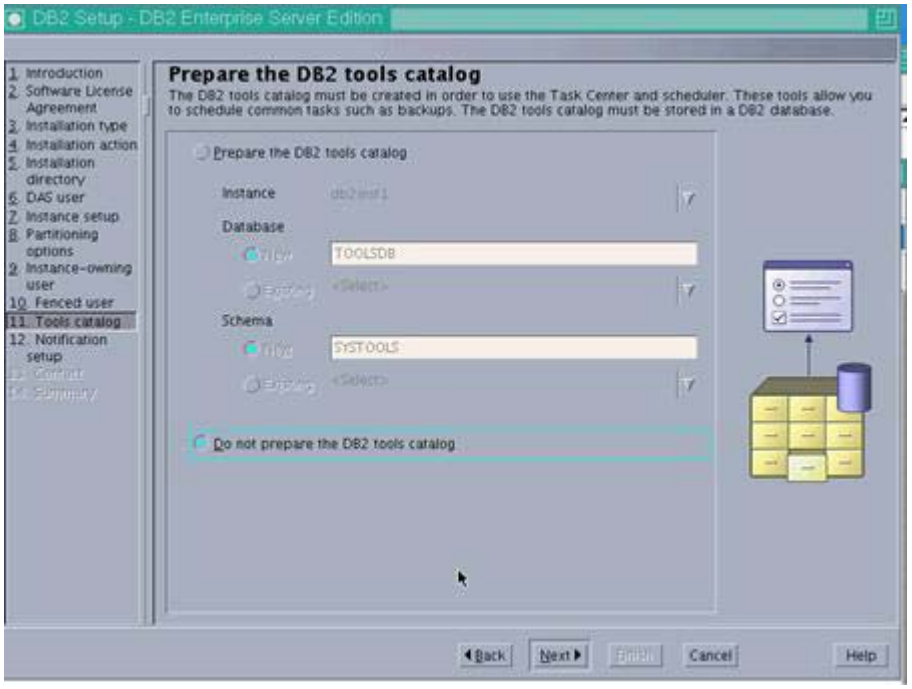


Figure 82. DB2 Setup wizard: Prepare the DB2 tools catalog

__ 13. Select **Do not set up your DB2 server to send notifications at this time**. Click **Next** to continue.

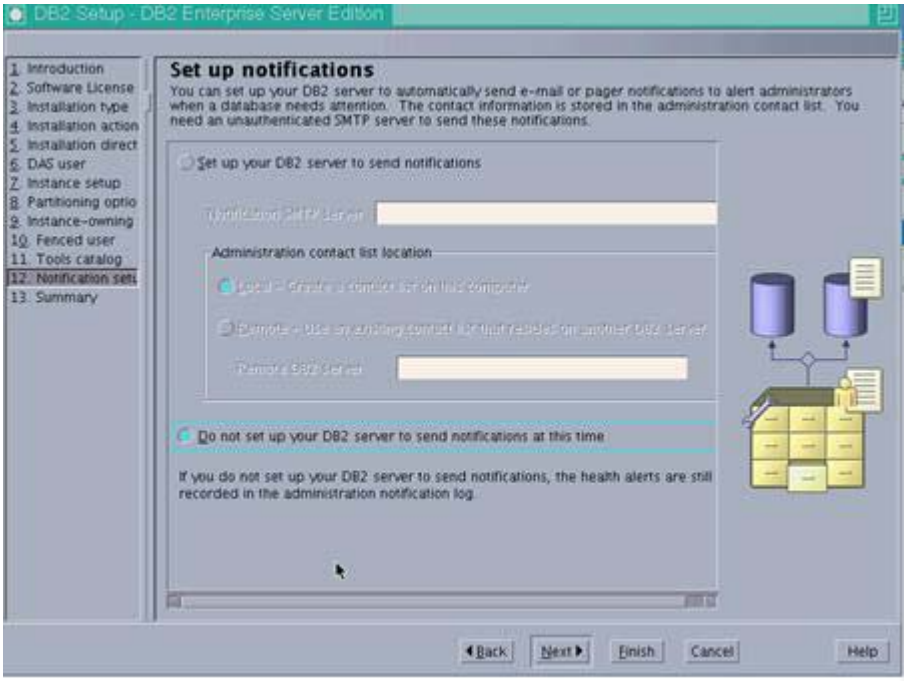


Figure 83. DB2 Setup wizard: Set up notifications

__ 14. Review the summary screen and finally click **Finish** to start the installation of the files onto the system.

Figure 84. DB2 Setup wizard: Summary: Start copying files (1 of 3)

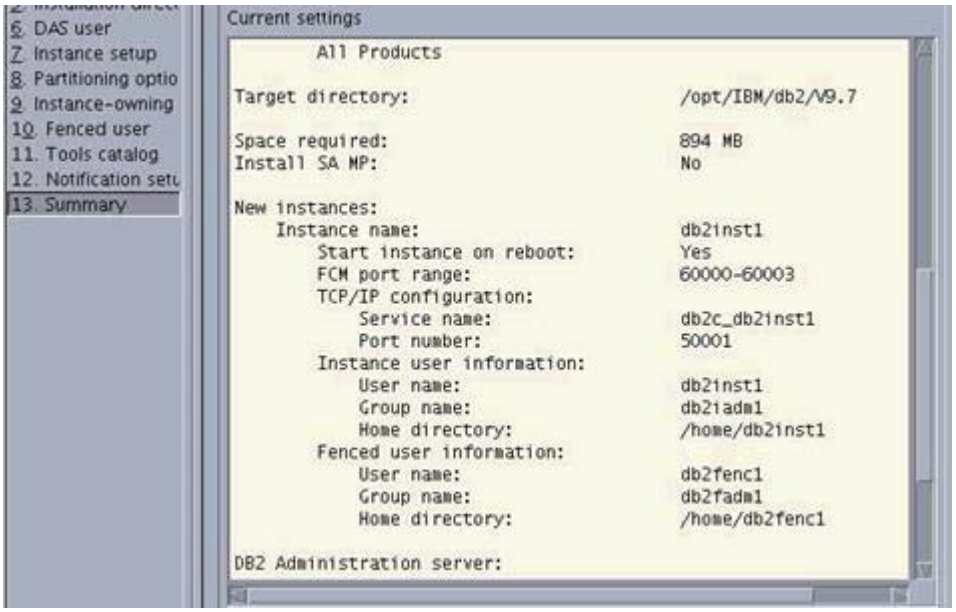


Figure 85. DB2 Setup wizard: Summary: Start copying files (2 of 3)

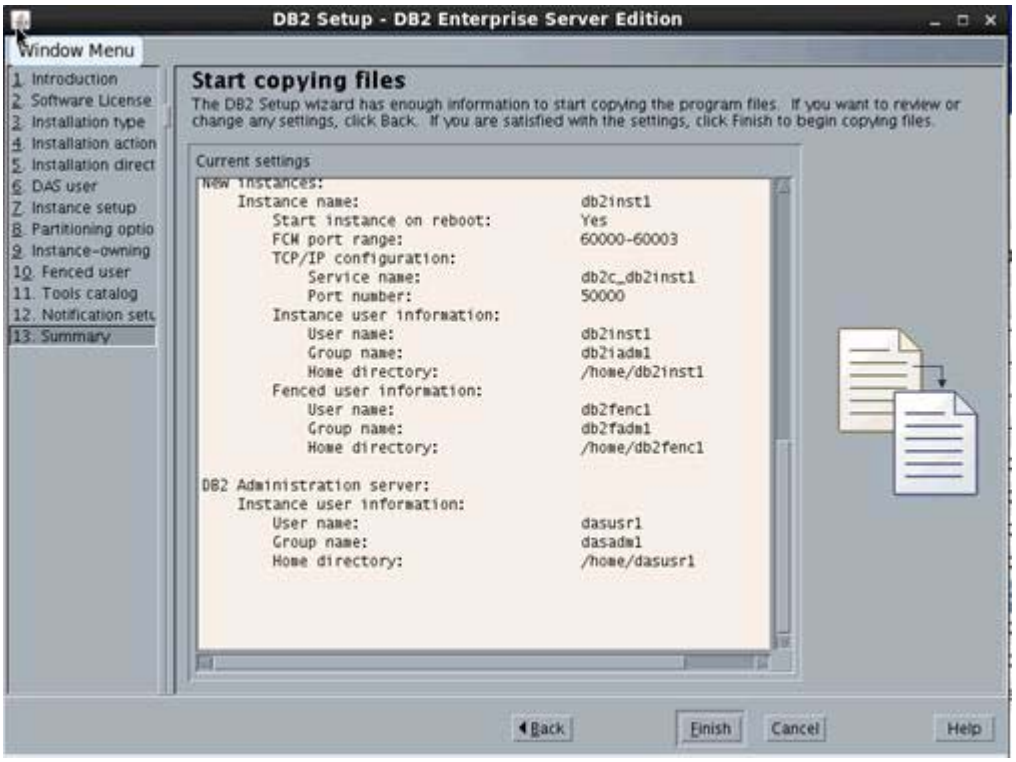


Figure 86. DB2 Setup wizard: Summary: Start copying files (3 of 3)

The installation begins.

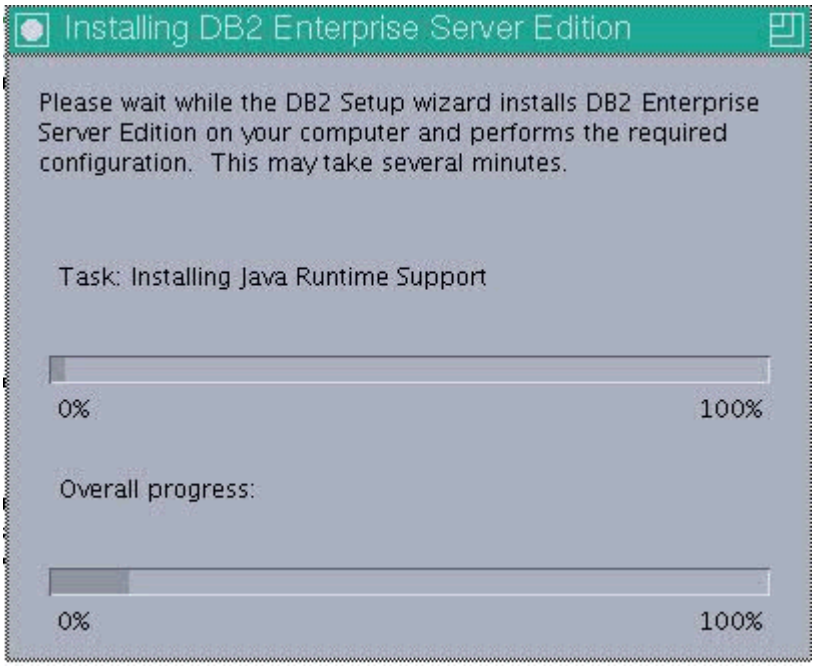


Figure 87. Installing DB2 Enterprise Server Edition

__ 15. After some time the installation successfully completes. Click **Finish** to close the installer.

__ 16. Verify the version of DB2 installed:

__ a. Open a terminal prompt.

__ b. Switch to the DB2 instance user, i. e. su - `db2inst1`.

__ c. Run the DB2 command `db2level` and you should see:

```
db2inst1@[redacted]:~> db2level
DB21085I  Instance "db2inst1" uses "64" bits and DB2 code release "SQL09070"
with level identifier "08010107".
Informational tokens are "DB2 v9.7.0.0", "s090521", "LINUXAMD6497", and Fix
Pack "0".
Product is installed at "/opt/IBM/db2/V9.7".

db2inst1@[redacted]:~>
```

Figure 88. DB2 command db2level

Apply the DB2 license to your server

__ 1. DB2 comes shipped with no license installed. To check it as user db2inst1, run the command `db2licm -l`.

```
db2inst1@[redacted]:~> db2start
[redacted] 15:00:34     0   0   SQL1026N  The database manager is already active
.
SQL1026N  The database manager is already active.
db2inst1@[redacted]:~> db2licm -l
Product name:                     "DB2 Enterprise Server Edition"
License type:                     "License not registered"
Expiry date:                      "License not registered"
Product identifier:               "db2ese"
Version information:              "9.7"
```

Figure 89. Command db2licm -l

You can see this reports License type = **"License not registered"**.

__ 2. To add the license to DB2, do the following steps:

__ a. Copy your license to the DB2 computer.

__ b. Run `db2licm -a <database license file>`.

```
db2inst1@[redacted]:~> db2licm -a /opt/software/DB2v9.7-64bit/db2ese_u.lic

LIC1402I  License added successfully.


LIC1426I  This product is now licensed for use as outlined in your License Agree
ment.  USE OF THE PRODUCT CONSTITUTES ACCEPTANCE OF THE TERMS OF THE IBM LICENSE
 AGREEMENT, LOCATED IN THE FOLLOWING DIRECTORY: "/opt/IBM/db2/V9.7/license/en_US
.iso88591"
```

Figure 90. Running db2licm -a <database license file>

__ 3. Run `db2licm -l` to verify that the license is added.

```
db2inst1@[redacted]:~> db2licm -l
Product name:                     "DB2 Enterprise Server Edition"
License type:                     "Authorized User Option"
Expiry date:                      "Permanent"
Product identifier:               "db2ese"
Version information:              "9.7"
Enforcement policy:               "Soft Stop"
Number of licensed authorized users: "25"
Features:
DB2 Performance Optimization ESE: "Not licensed"
DB2 Storage Optimization:         "Not licensed"
DB2 Advanced Access Control:      "Not licensed"
DB2 Geodetic Data Management:     "Not licensed"
IBM Homogeneous Replication ESE:  "Not licensed"
```

Figure 91. Running db2licm -l

IBM Tivoli Directory Integrator 7.1 installation

The installation of Tivoli Directory Integrator is needed so that the profiles DB can be populated with LDAP information.

__ 1. Copy the Tivoli Directory Integrator 7.1 installer to your computer and extract it.

__ 2. From a VNC: Terminal prompt run the Tivoli Directory Integrator installer: `./install_tdiv71_linux_x86_64.bin`. You should see the following screen. Select **English** as your Language and click **ok**.

Figure 92. IBM Tivoli Directory Integrator v7.1

__ 3. Click **Next** in the Introduction screen.

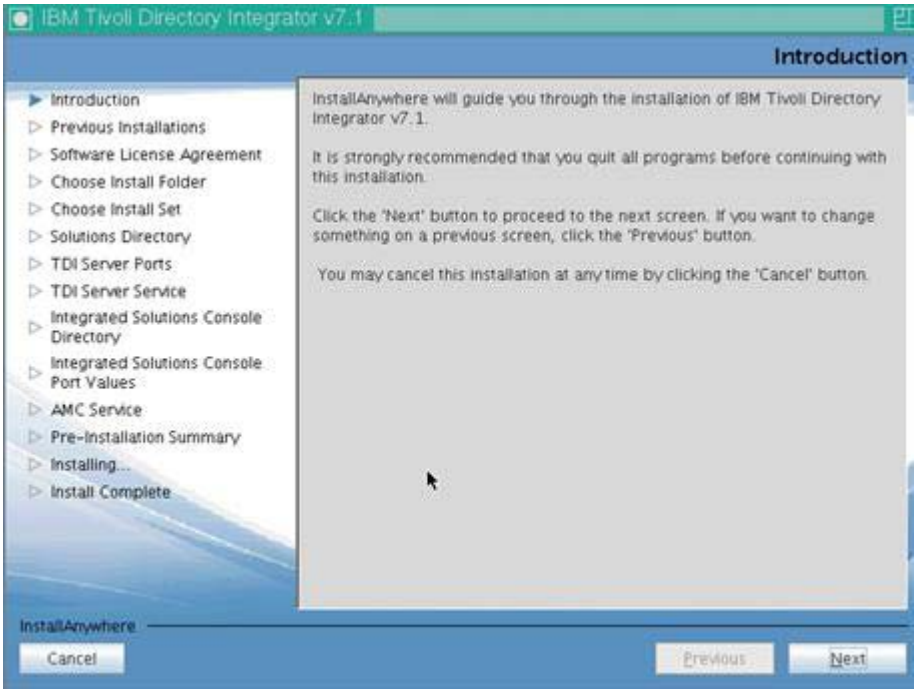


Figure 93. IBM Tivoli Directory Integrator v7.1: Welcome

__ 4. The installation searches to see whether Tivoli Directory Integrator is already installed. Click **Next**.

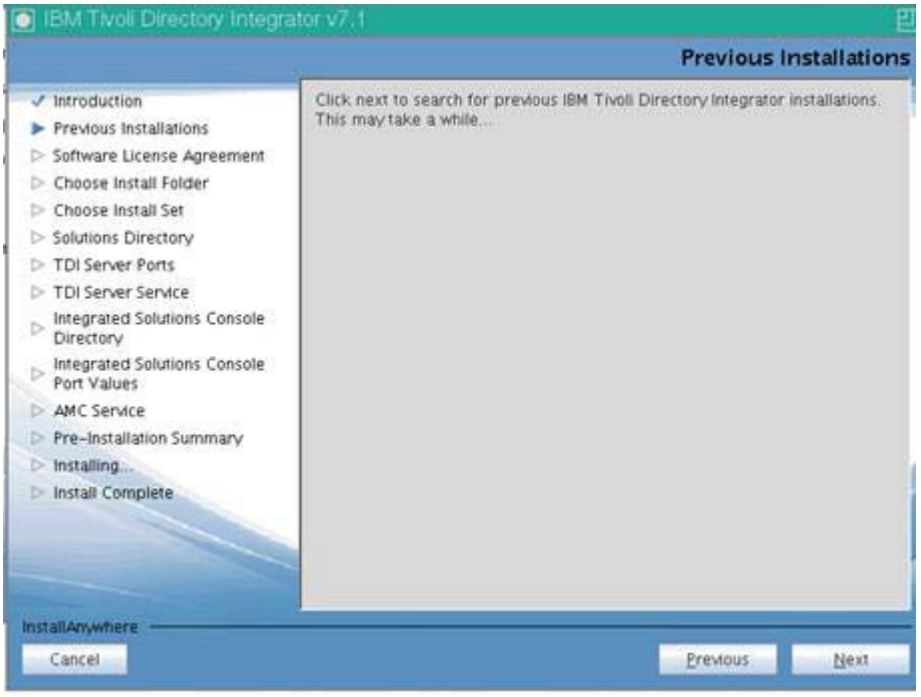


Figure 94. IBM Tivoli Directory Integrator v7.1: Previous installations

__ 5. After some time it finishes. Accept the license agreement and click **Next** to continue.

Figure 95. IBM Tivoli Directory Integrator v7.1: Software License Agreement

__ 6. Change the path to where Tivoli Directory Integrator should install. Click **Next** to continue.

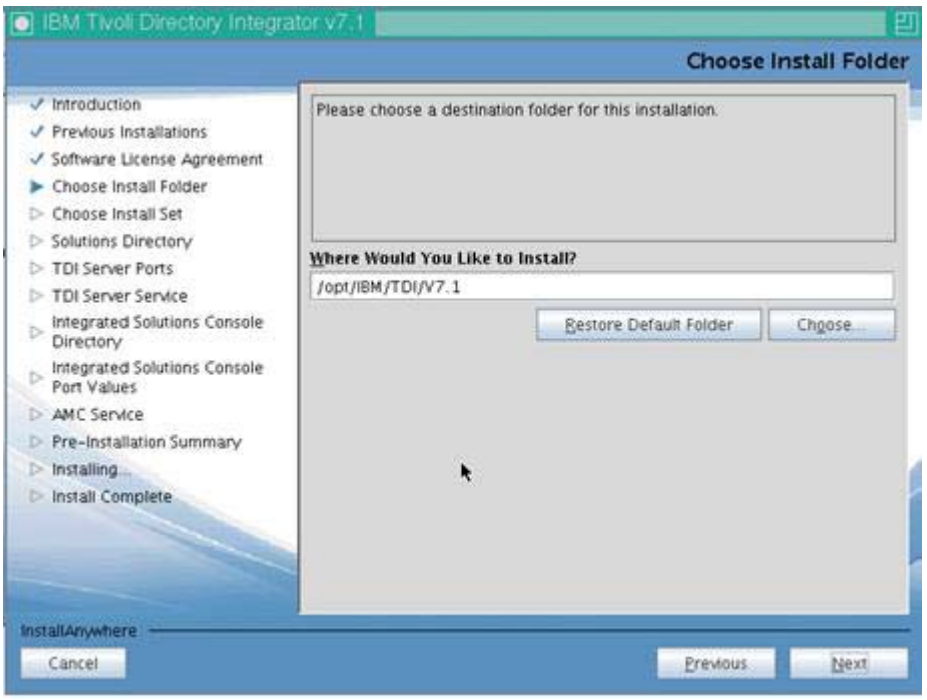


Figure 96. IBM Tivoli Directory Integrator v7.1: Choose Install Folder

__ 7. Choose the **Typical** installation type and click **Next** to continue.

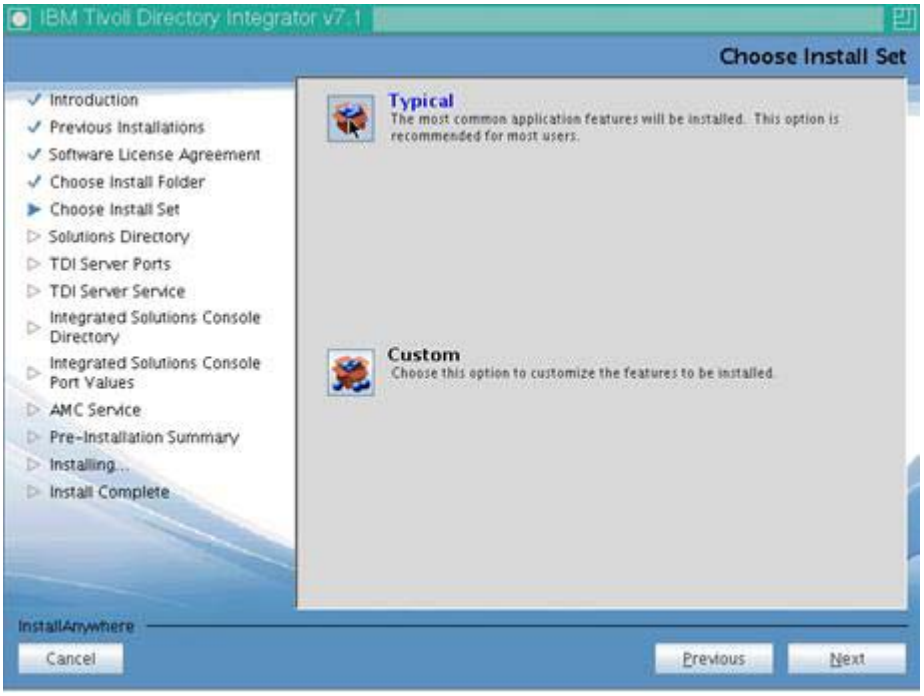


Figure 97. IBM Tivoli Directory Integrator v7.1: Choose Install Set

__ 8. Select the option “Do not specify” and click **Next** to continue.

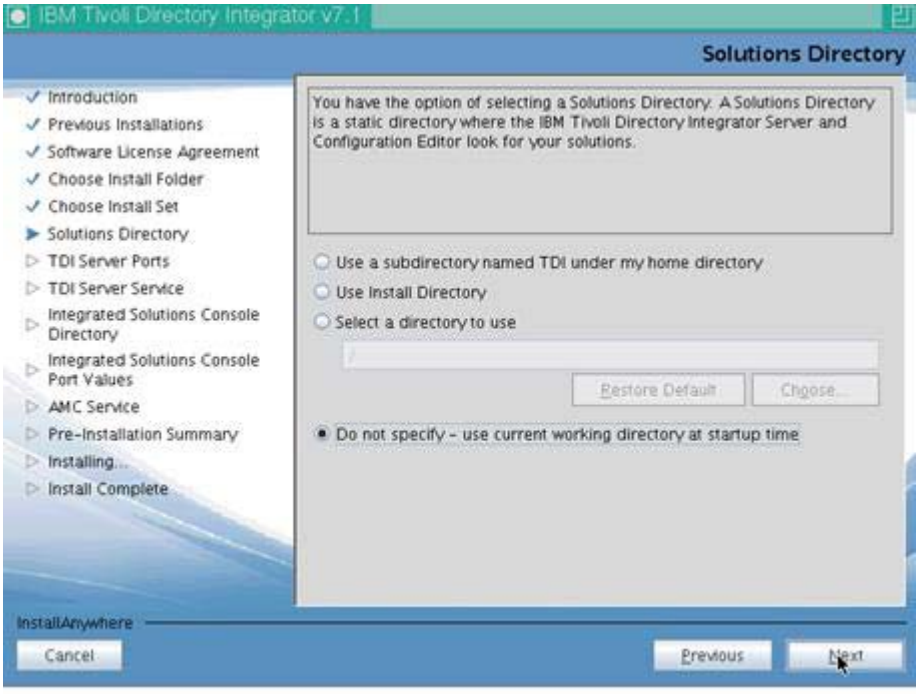


Figure 98. IBM Tivoli Directory Integrator v7.1: Solutions Directory

__ 9. Use the default ports and click **Next** to continue.

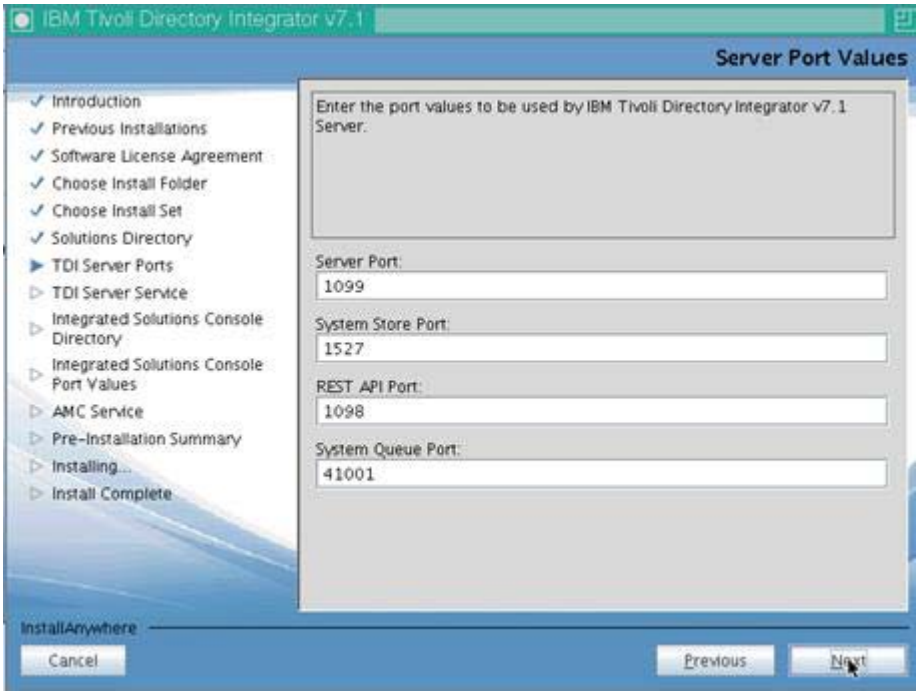


Figure 99. IBM Tivoli Directory Integrator v7.1: Server Port Values

__ 10. Do not select “Register as a system service”. Click **Next** to continue.

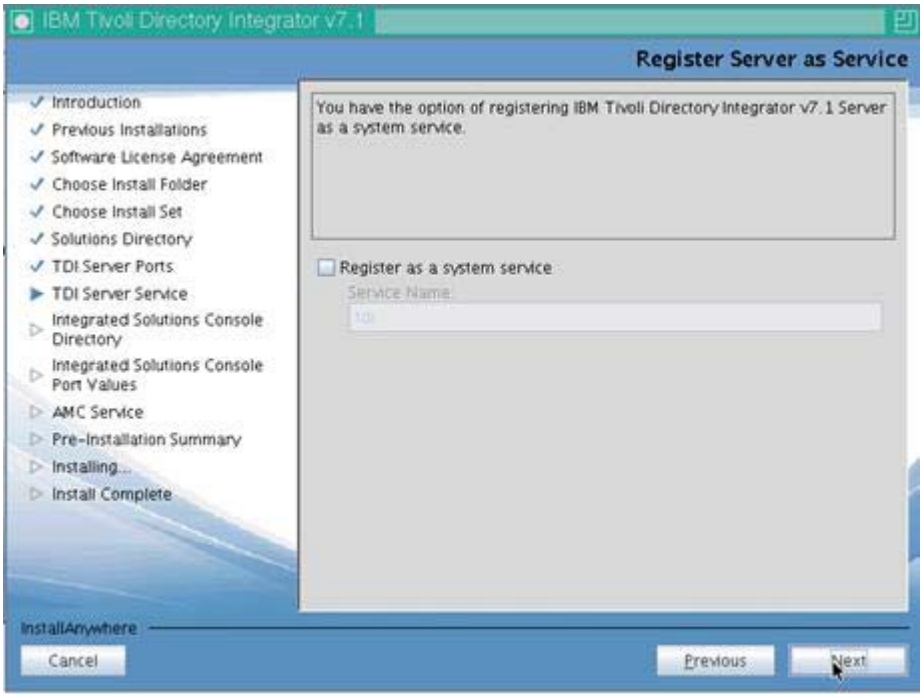


Figure 100. IBM Tivoli Directory Integrator v7.1: Register Server as Service

__ 11. Use the default ports and select **Next** to continue.

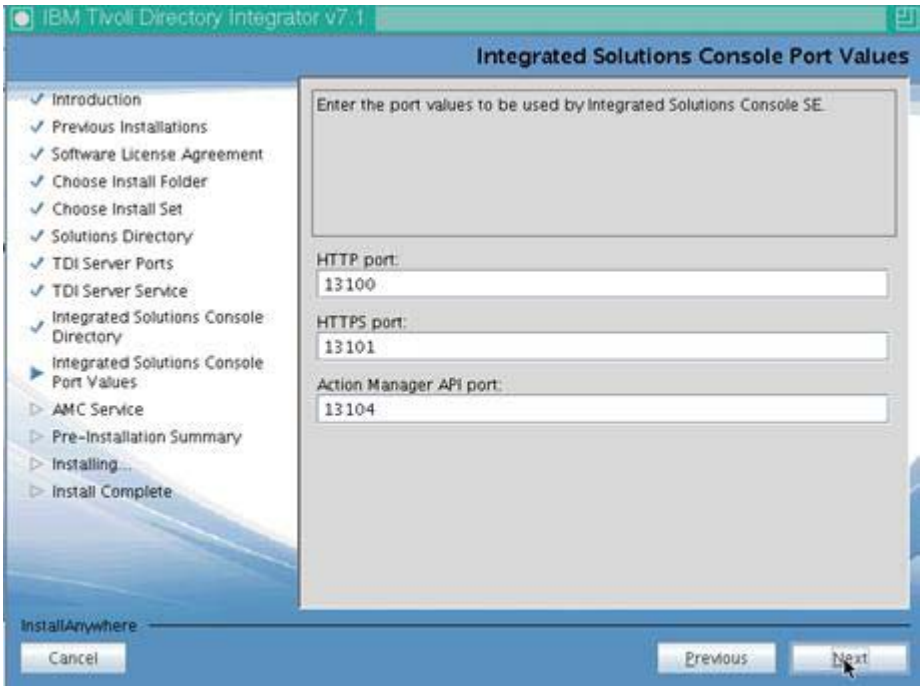


Figure 101. IBM Tivoli Directory Integrator v7.1: Integrated Solutions Console Port Values

__ 12. Do not select “Register as a system service”. Click **Next** to continue.

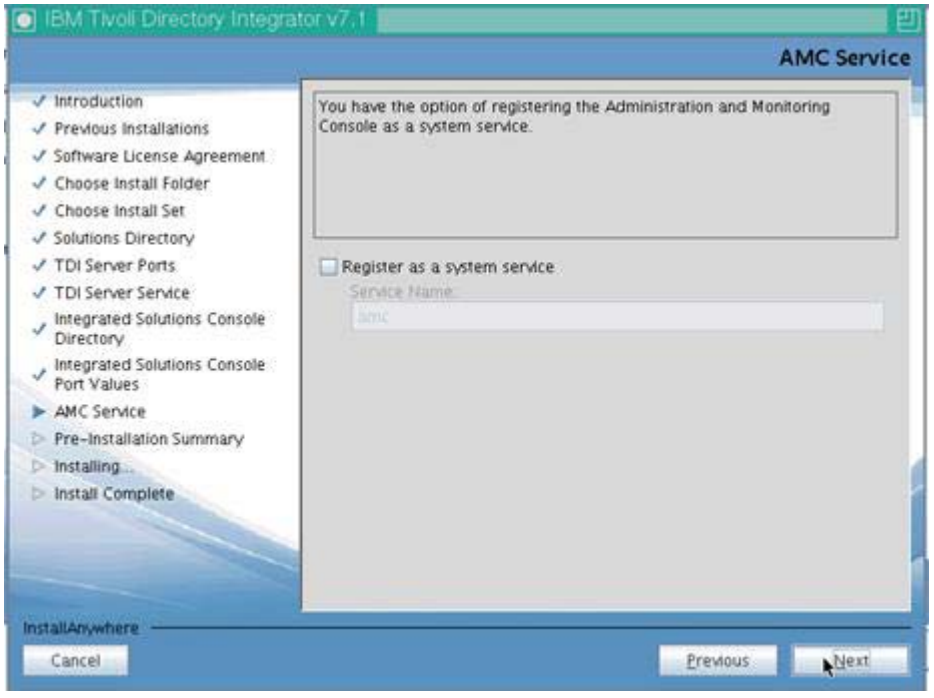


Figure 102. IBM Tivoli Directory Integrator v7.1: AMC Service

__ 13. A pre-installation summary screen displays. Click **Install** to start the installation.

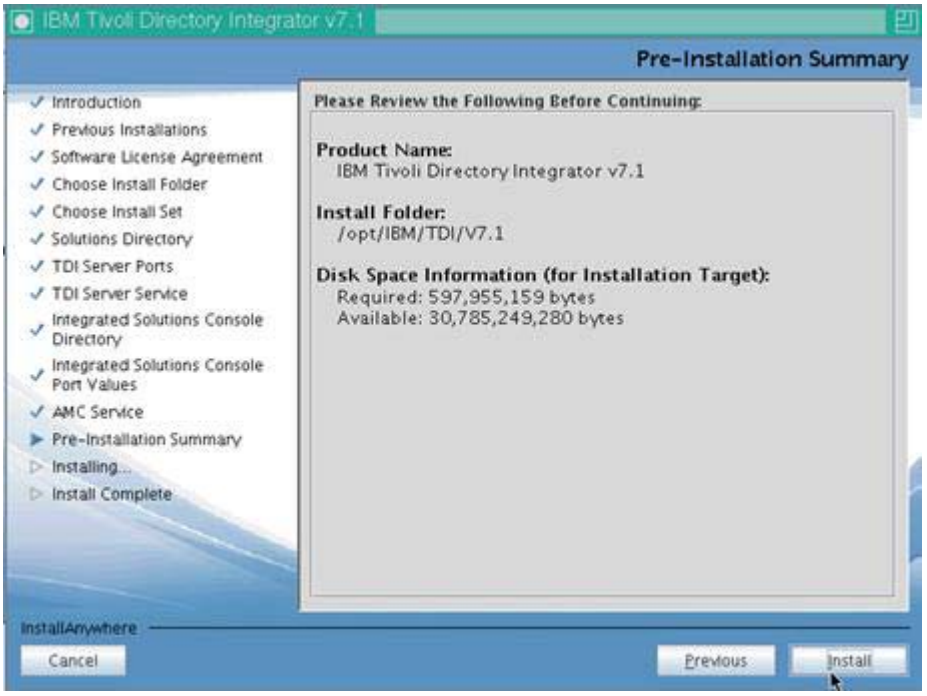


Figure 103. IBM Tivoli Directory Integrator v7.1: Pre-installation Summary

The install begins.

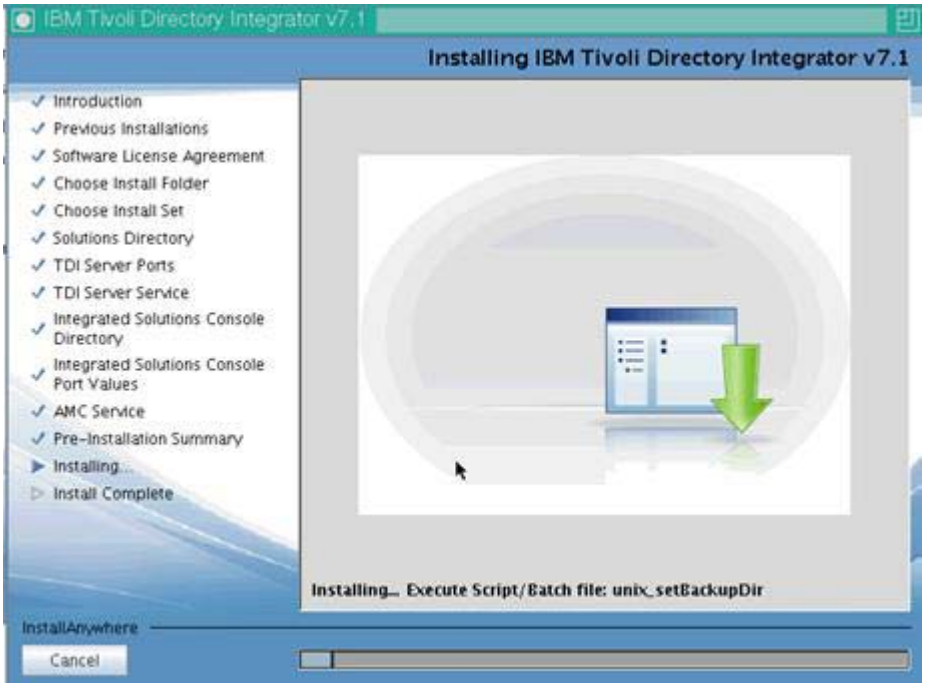


Figure 104. Installing IBM Tivoli Directory Integrator v7.1

__ 14. After some time the installation finishes. Clear the “Start Configuration Editor” option and click **Done** to close the installer.

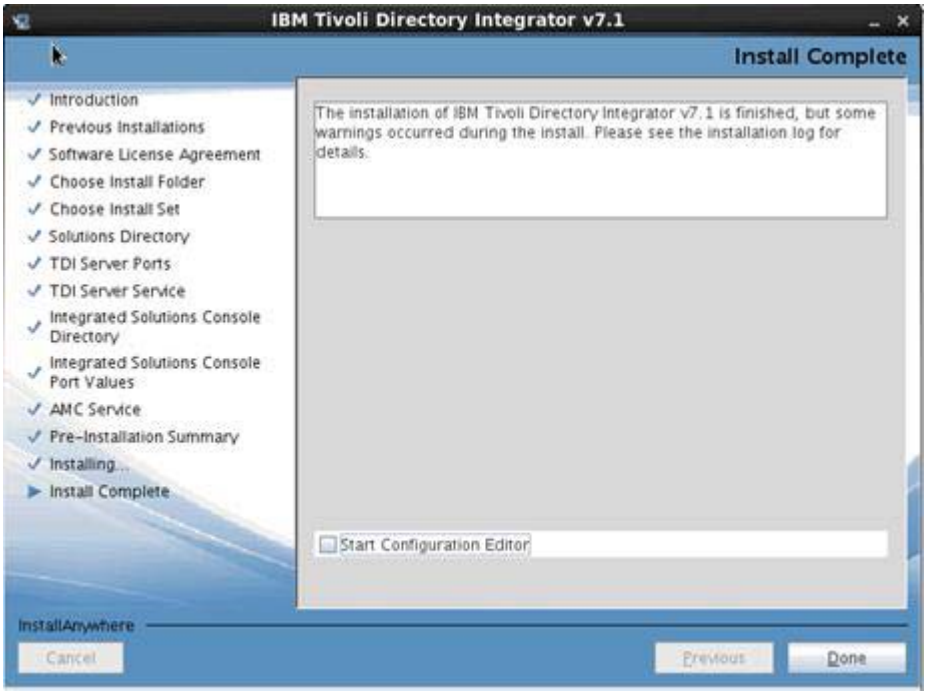


Figure 105. IBM Tivoli Directory Integrator v7.1: Installation Complete

Tivoli Directory Integrator 7.1 is installed. Now you install FP5 on top of it.

IBM Tivoli Directory Integrator 7.1 FixPack 5 installation

__ 1. Copy the fix pack to a location on your system and extract it.

__ 2. Make sure Tivoli Directory Integrator is not running before applying the fix pack.

__ 3. Then, go to `/opt/IBM/TDI/V7.1/bin` and run the following command: `./applyUpdates.sh -update /opt/software/TDI/TDI 7.1/7.1.0-TIV-TDI-FP0005/TDI-7.1-FP0005.ZIP/`.

Note

Run this command from a VNC Session.

The FixPack is then installed.

```
[root@dslvm65 bin]# ./applyUpdates.sh -update /software/TDI7.1/7.1.0-TIV-TDI-FP0
005/TDI-7.1-FP0005.zip
./applyUpdates.sh: line 57: -Dlog4j.configuration=file:/opt/IBM/TDI/V7.1/etc/upd
ateinstaller-log4j.properties: No such file or directory
log4j:WARN No appenders could be found for logger (UpdateInstaller.UpdateInstall
erMsgs).
log4j:WARN Please initialize the log4j system properly.
CTGDK0023I Applying fix 'TDI-7.1-FP0005' using backup directory '/opt/IBM/TDI/V7
.1/maintenance/BACKUP/TDI-7.1-FP0005'.
CTGDK0027I Updating SERVER.
CTGDK0027I Updating CE.
CTGDK0027I Updating EXAMPLES.
```

Figure 106. Installing FixPack

__ 4. Check that the installation was OK and run `./applyUpdates.sh -queryreg`. You should see this result:

```
[root@dslvm65 bin]# ./applyUpdates.sh -queryreg
./applyUpdates.sh: line 57: -Dlog4j.configuration=file:/opt/IBM/TDI/V7.1/etc/updateinstaller-log4j.properties: No such file o
r directory
log4j:WARN No appenders could be found for logger (UpdateInstaller.UpdateInstallerMsgs).
log4j:WARN Please initialize the log4j system properly.
Information from .registry file in: /opt/IBM/TDI/V7.1
Edition: Identity
Level: 7.1.0.5
License: None

Fixes Applied
=============
TDI-7.1-FP0005(7.1.0.0)

Components Installed
====================
BASE
SERVER
   -TDI-7.1-FP0005
CE
   -TDI-7.1-FP0005
JAVADOCS
EXAMPLES
   -TDI-7.1-FP0005
EMBEDDED WEB PLATFORM
AMC
   Deferred: false

[root@dslvm65 bin]#
```

Figure 107. Checking if the installation was successful

__ 5. Make the following DB2 libraries available to Tivoli Directory Integrator by copying the files `db2jcc.jar` and `db2jcc_license_cu.jar` from the DB2 `java` subdirectory (`/opt/ibm/db2/V9.7/java`) to the Tivoli Directory Integrator `ext` directory (for example, `/opt/IBM/TDI/V7.1/jvm/jre/lib/ext`).

```
dalvm1010:/opt/IBM/TDI/V7.1/jvm/jre/lib/ext # ls
cmpCrmf.jar                 db2jcc.jar            dtfj-interface.jar  gskikm.jar          ibmjceffips.jar     ibmpkcs11impl.jar     jaccess.jar     xmlencfw.jar
IBMKeyManagementServer.jar  db2jcc_license_cu.jar dtfj.jar            healthcenter.jar    ibmjceprovider.jar  ibmsaslprovider.jar   jdmpview.jar
JavaDiagnosticsCollector.jar dtmme.jar            dtfjview.jar        ibmmqprovider.jar   ibmkeycert.jar      ibmxmlencprovider.jar localmdata.jar
dalvm1010:/opt/IBM/TDI/V7.1/jvm/jre/lib/ext #
```

Figure 108. Making DB2 libraries available

4. Create Connections databases on DB2 server by using the dbWizard

__ 1. Log in to your database server as the `root` user or system administrator.

__ 2. Grant display authority to all users by running the following commands under the root user or system administrator:

xhost + // Grant display authority to other users

echo $DISPLAY // Echo the value of DISPLAY under the root user

__ 3. Ensure that the current user is qualified or else switch to a qualified user by running the following commands. Switch to the db2 admin (in this case the db2 admin is `db2inst1`)

su - db2inst1

export DISPLAY=<hostname:displaynumber.screennumber> where <hostname:displaynumber.screennumber> represents the client system, monitor number, and window number.

export DISPLAY=:1.0

__ 4. Start the database instance; enter: `db2start`.

__ 5. Use the dbWizard to create the Connections databases:

__ a. First, switch to the db2 admin user: `db2inst1`.

__ b. Copy the `IBM_Connection40_Wzd_LNXAIX_CIA3HML.tar` to your computer and extract it.

__ 6. Next, as `db2inst1`, run `./dbWizard.sh` to start the database wizard for IBM Connections 4.0.

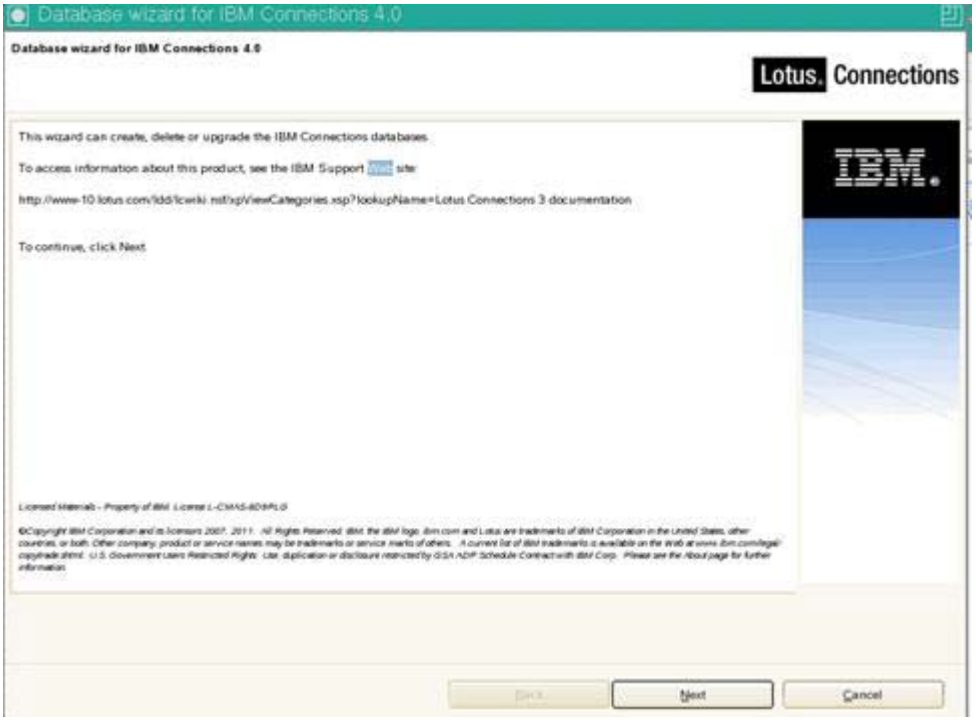


Figure 109. Database wizard for IBM Connections 4.0

__ 7. Select **Create** and then **Next** to continue.

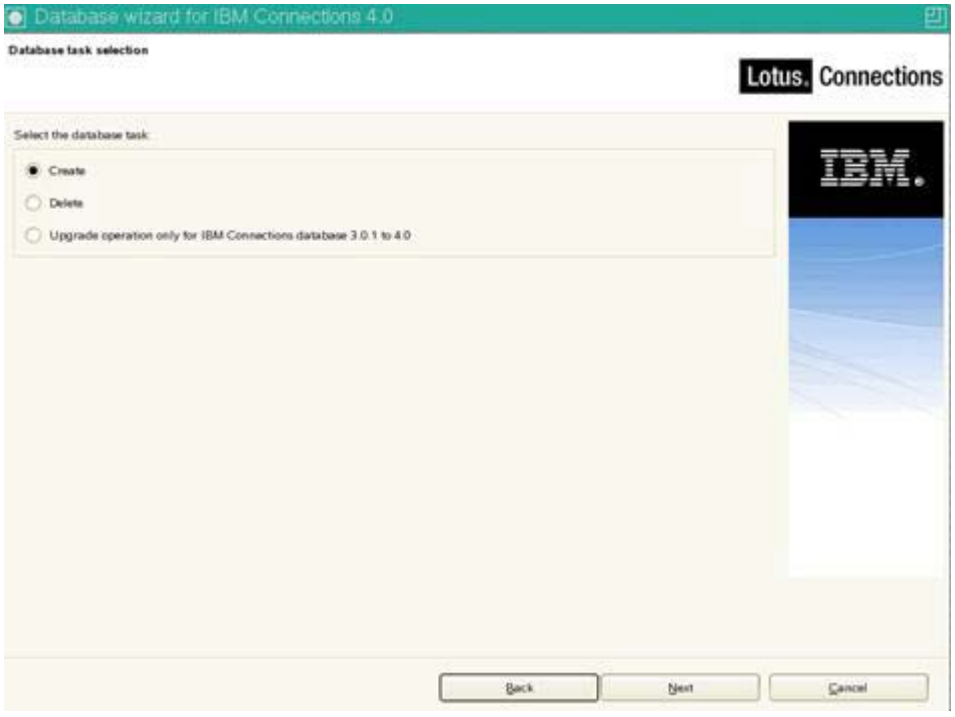


Figure 110. Database wizard for IBM Connections 4.0: Database task selection

__ 8. Select the path for your database installation location and the database instance name. Click **Next** to continue.

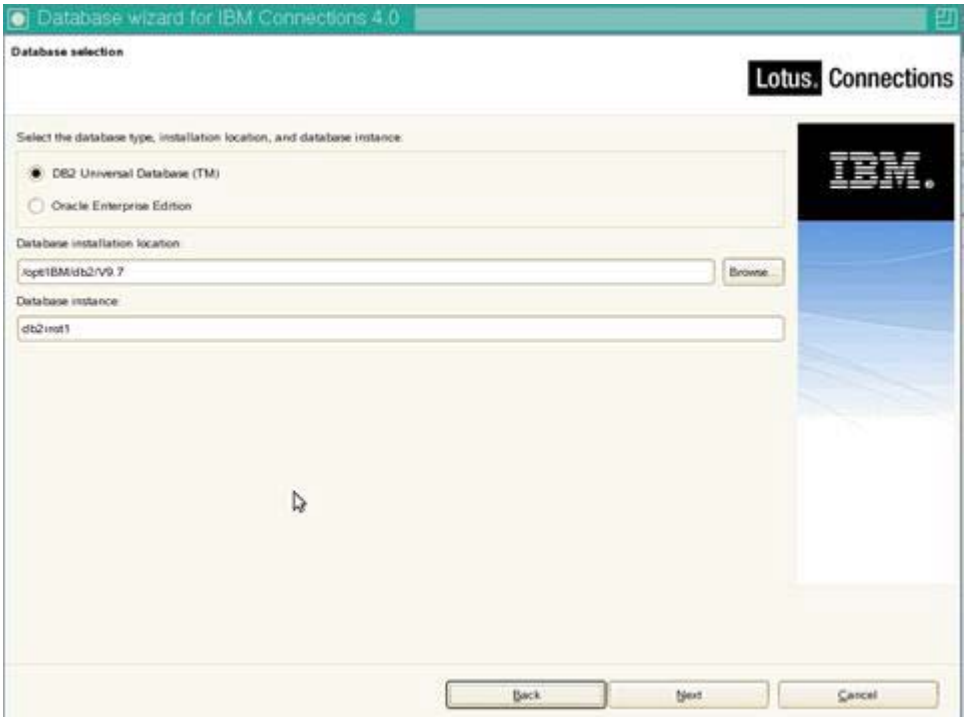


Figure 111. Database wizard for IBM Connections 4.0: Database selection

__ 9. Ensure that all databases are selected and then click **Next** to continue.

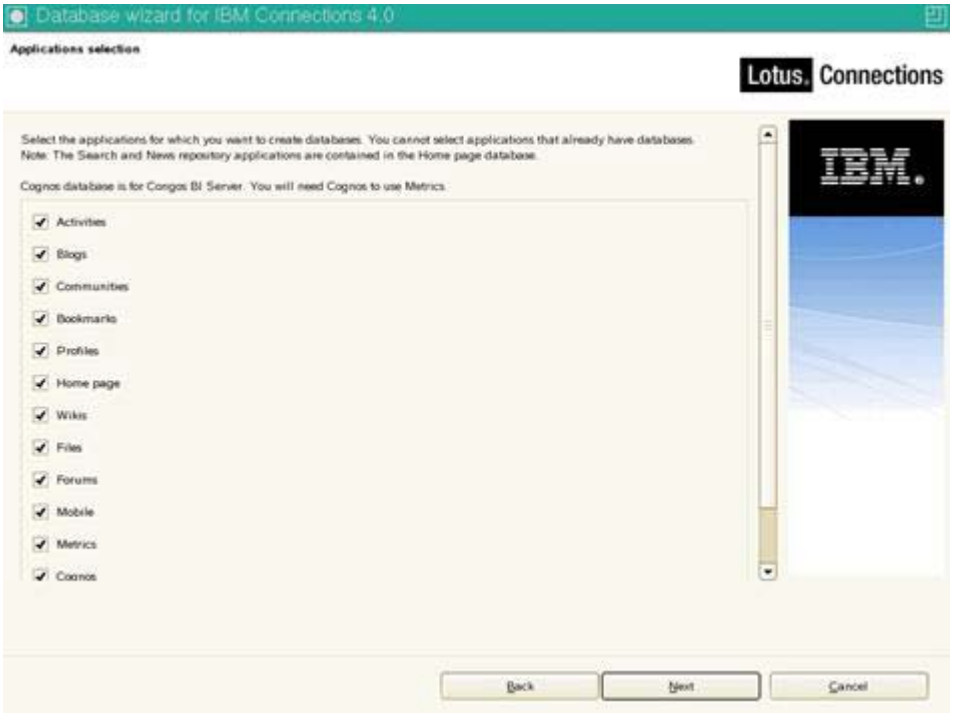


Figure 112. Database wizard for IBM Connections 4.0: Applications selection

__ 10. Click **Create** in the summary screen.

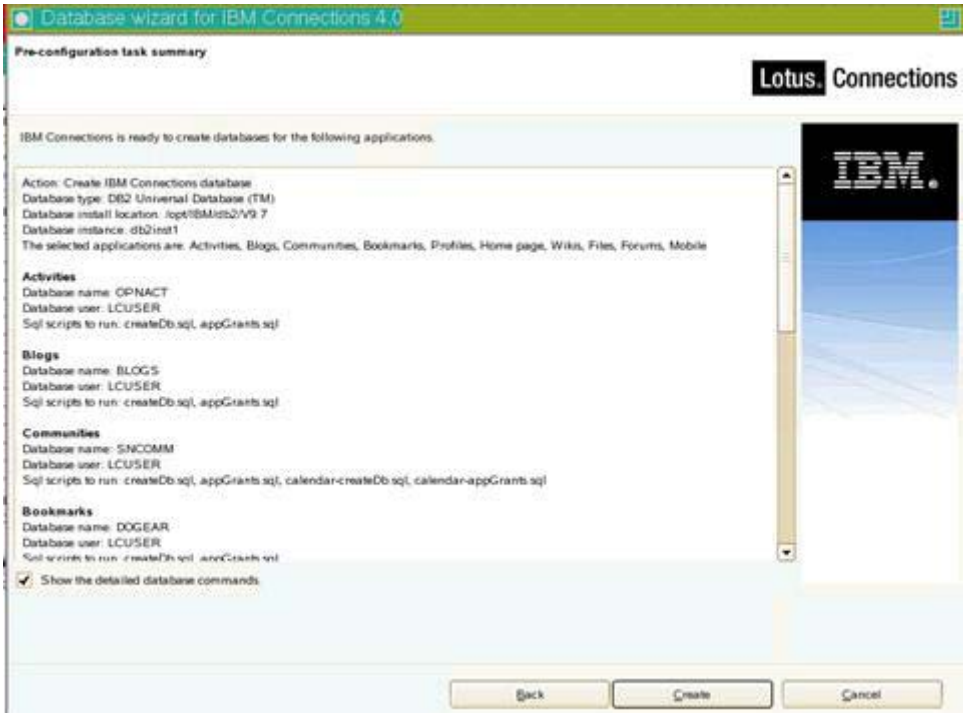


Figure 113. Database wizard for IBM Connections 4.0: Pre-configuration task summary

__ 11. Finally, click **Execute** to create the databases.

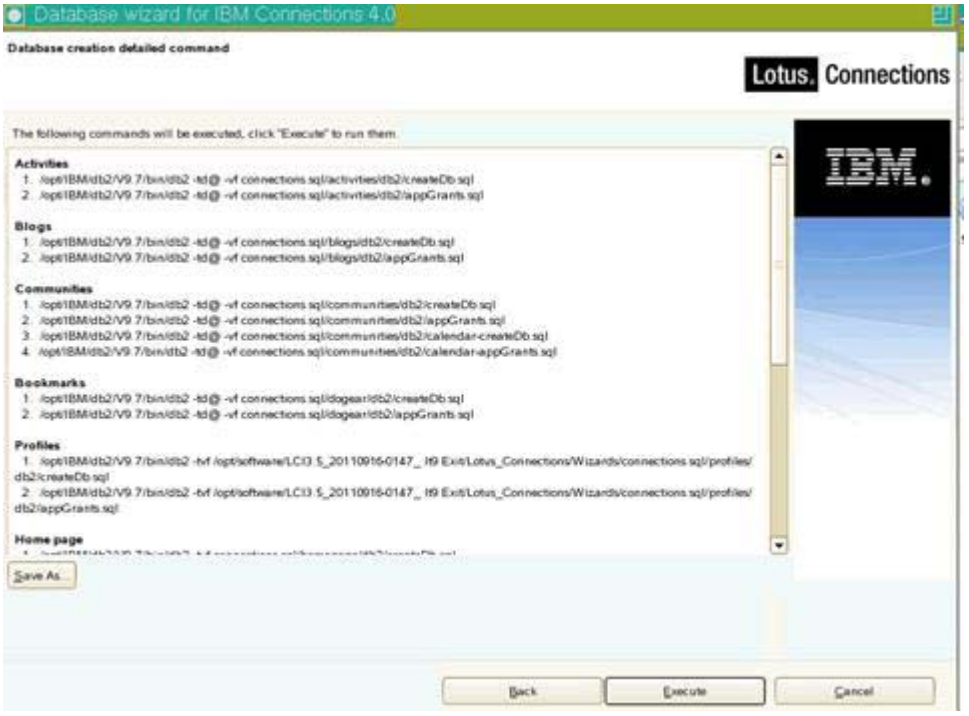


Figure 114. Database wizard for IBM Connections 4.0: Database creation detailed command

The databases are being created.

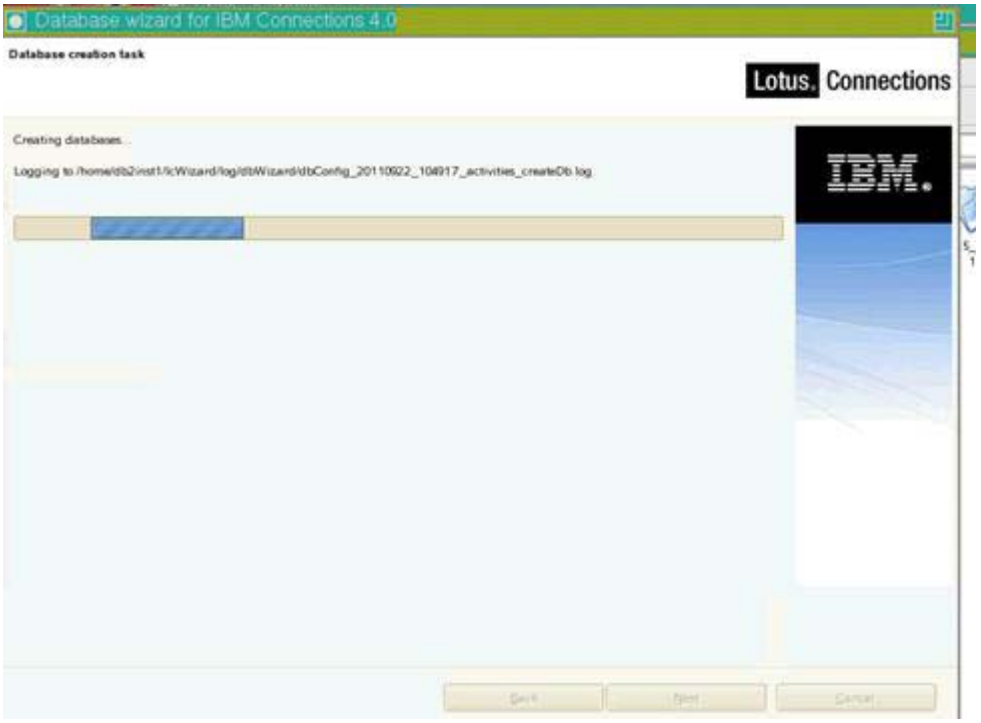


Figure 115. Database wizard for IBM Connections 4.0: Database creation task

__ 12. After some time, the databases are created. Click **Finish**.

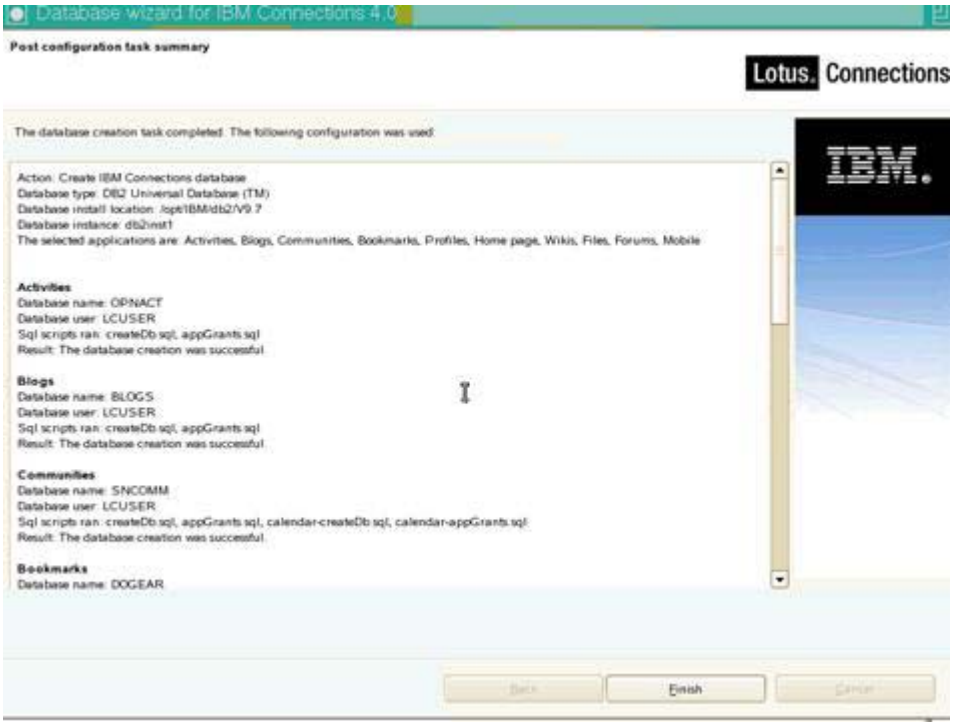


Figure 116. Database wizard for IBM Connections 4.0: Post configuration task summary

If you now run the db2 command: db2 `list database directory`, you should see that all databases are created.

5. Populate the Profiles database with LDAP user information

__ 1. As `root`, copy the `IBM_Connection40_Wzd_LNXAIX_CIA3HML.tar` to your DB2 computer and extract it.

__ 2. Go to the Wizard folder and, as `root`, run `./populationWizard.sh` and on the Welcome page of the wizard click **Next** to continue.

Figure 117. Profiles population wizard for IBM Connections 4.0: Welcome

__ 3. Enter the location of Tivoli Directory Integrator and then click **Next**.

Note

This page is shown only if the wizard cannot automatically detect your Tivoli Directory Integrator directory.

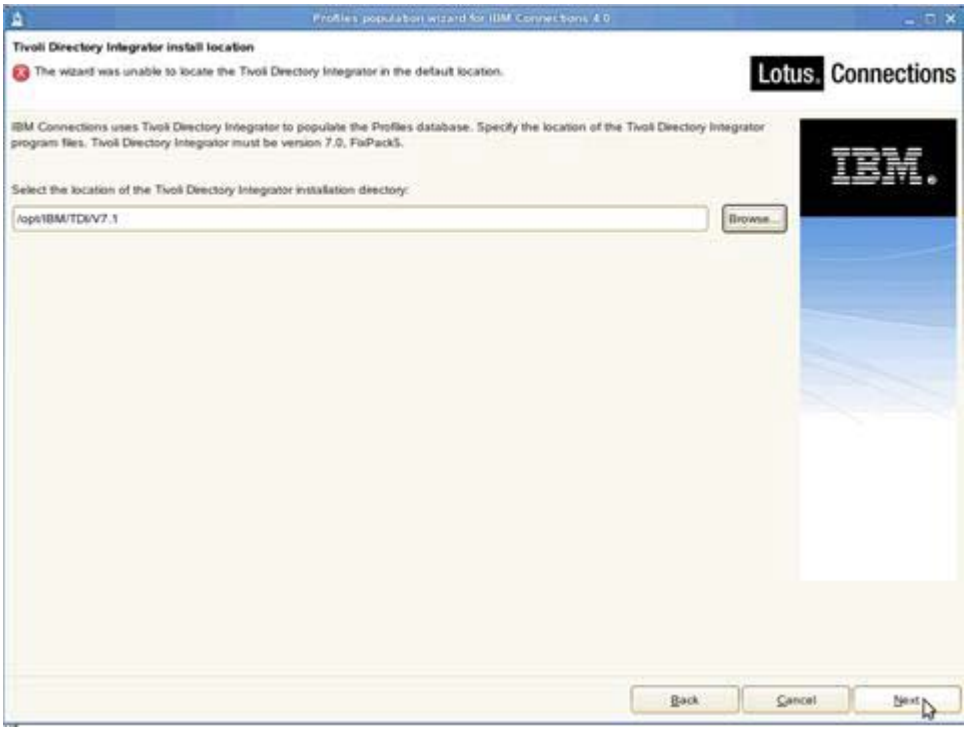


Figure 118. Profiles population wizard for IBM Connections 4.0: Tivoli Directory Integrator installation location

__ 4. Select **DB2 Universal Database** and click **Next**.

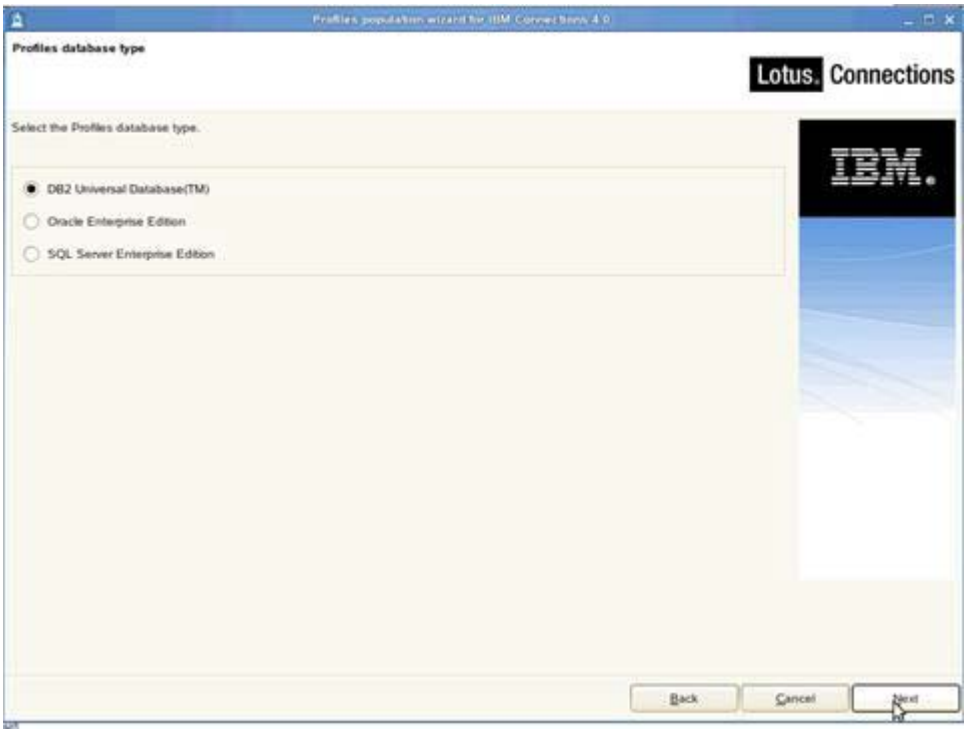


Figure 119. Profiles population wizard for IBM Connections 4.0: Profiles database type

__ 5. Next, enter the database information for where your PEOPLEDB database is located and click **Next** to continue.

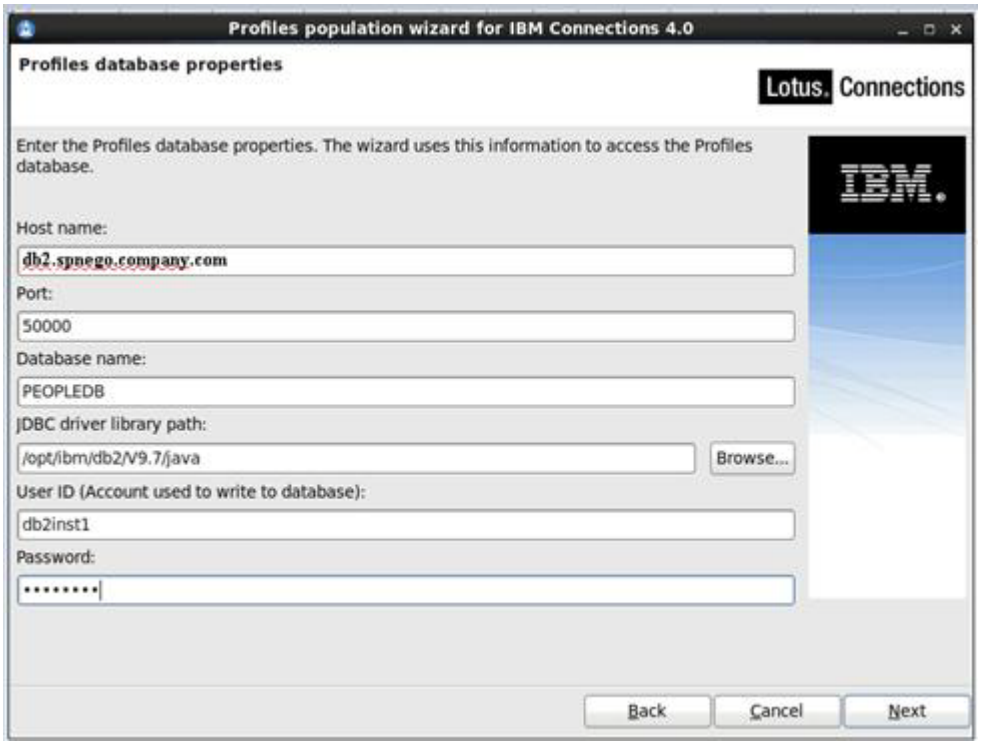


Figure 120. Profiles population wizard for IBM Connections 4.0: Profiles database properties

__ 6. Enter the LDAP server and port number and then click **Next** to continue.

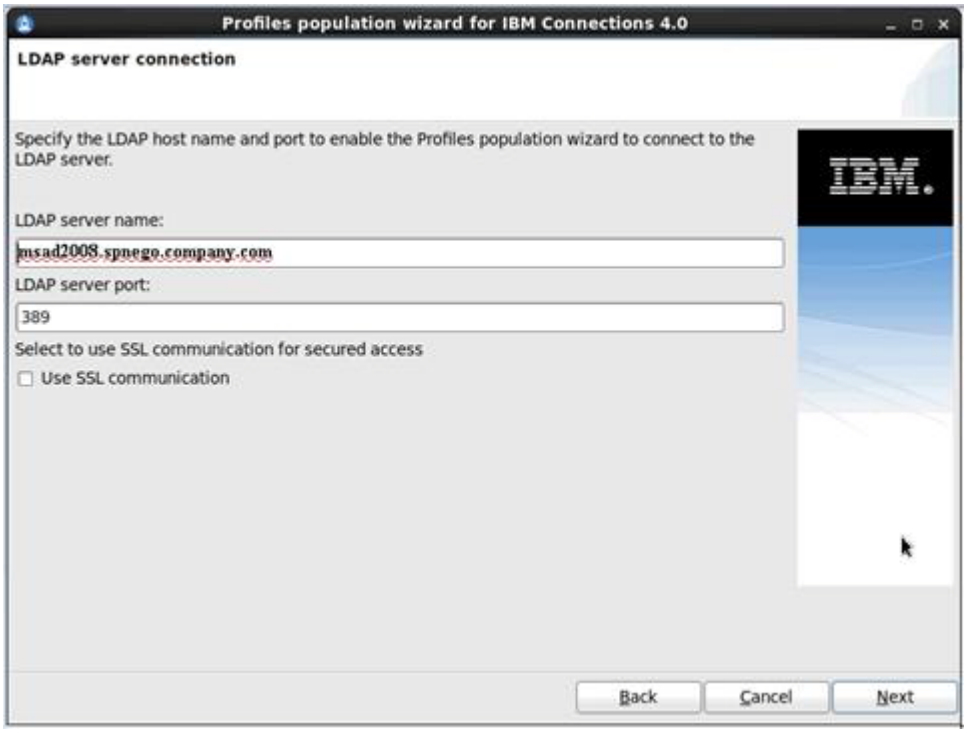


Figure 121. Profiles population wizard for IBM Connections 4.0: LDAP server connection

__ 7. Enter the bind user details and password and click **Next** to continue.

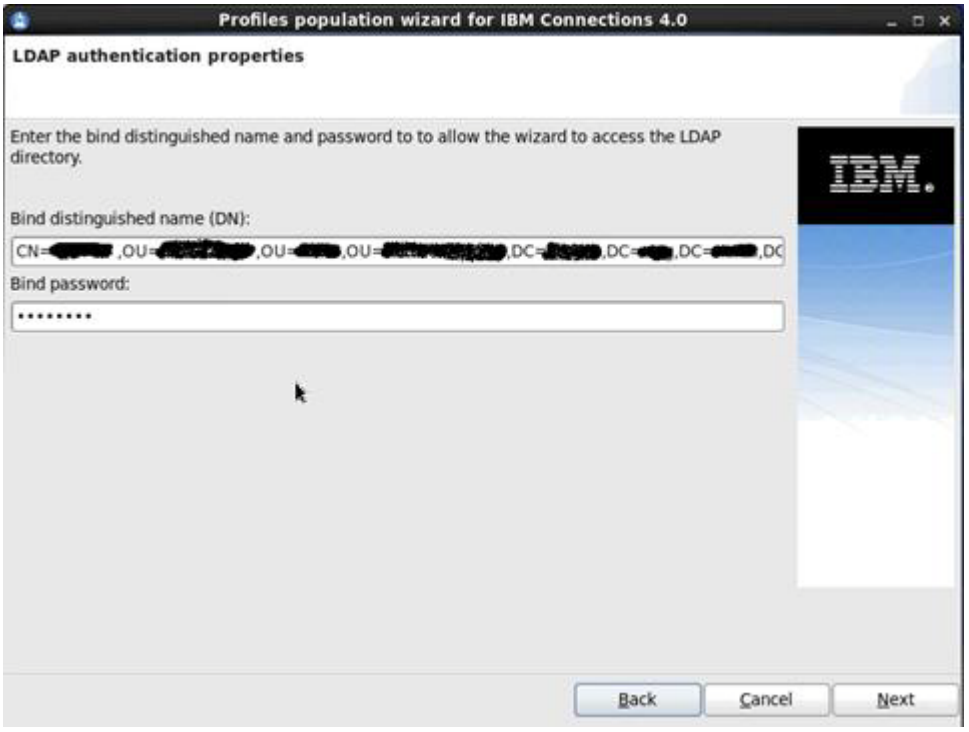


Figure 122. Profiles population wizard for IBM Connections 4.0: LDAP authentication properties

__ 8. Enter the search base and search filter. Click **Next** to continue.

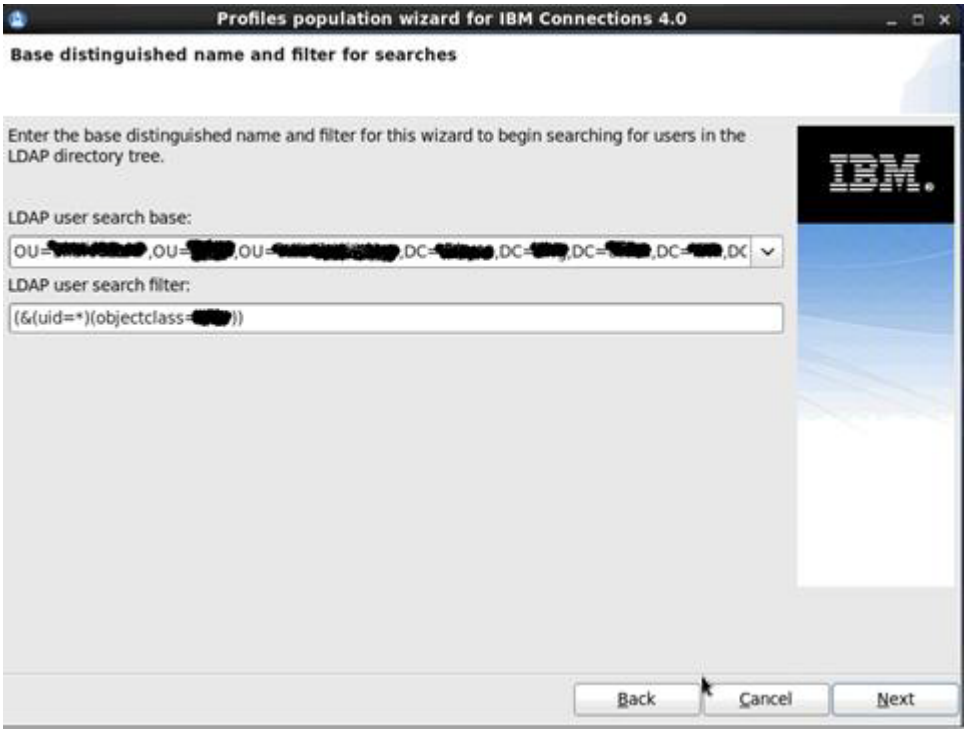


Figure 123. Profiles population wizard for IBM Connections 4.0: Base distinguished name and filter for searches

__ 9. Use the default database mappings. Click **Next** to continue.

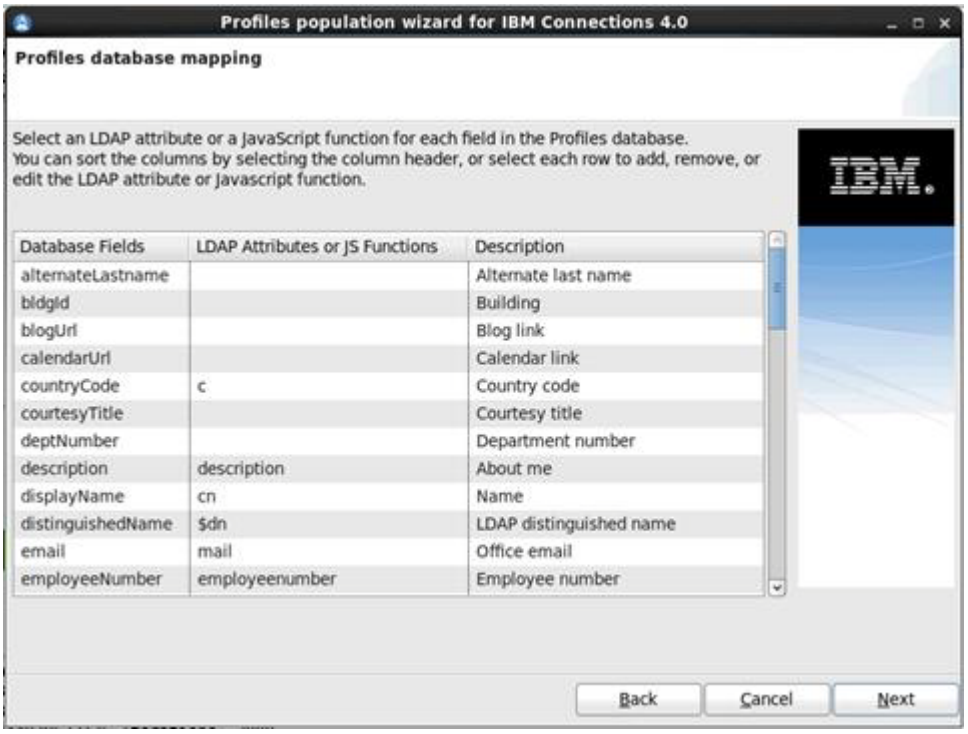


Figure 124. Profiles population wizard for IBM Connections 4.0: Profiles database mapping

__ 10. Do not select any of the **Optional database tasks**.

__ 11. Select **Yes** for “Do you want to run the task that marks the profiles of each manager?”.

__ 12. Click **Next** to continue.

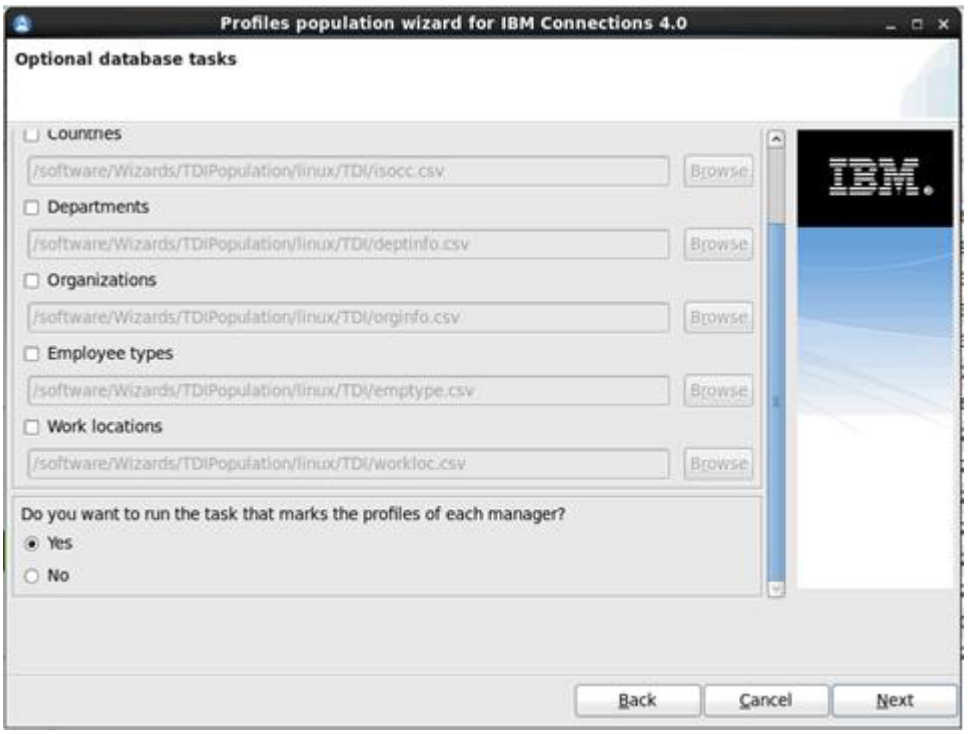


Figure 125. Profiles population wizard for IBM Connections 4.0: Optional database tasks

__ 13. Review the summary page to ensure that the information you entered in the previous panels is correct.

__ 14. To make changes, click **Back** to return to the relevant page and edit the information. Otherwise, click **Configure** to begin populating the database.

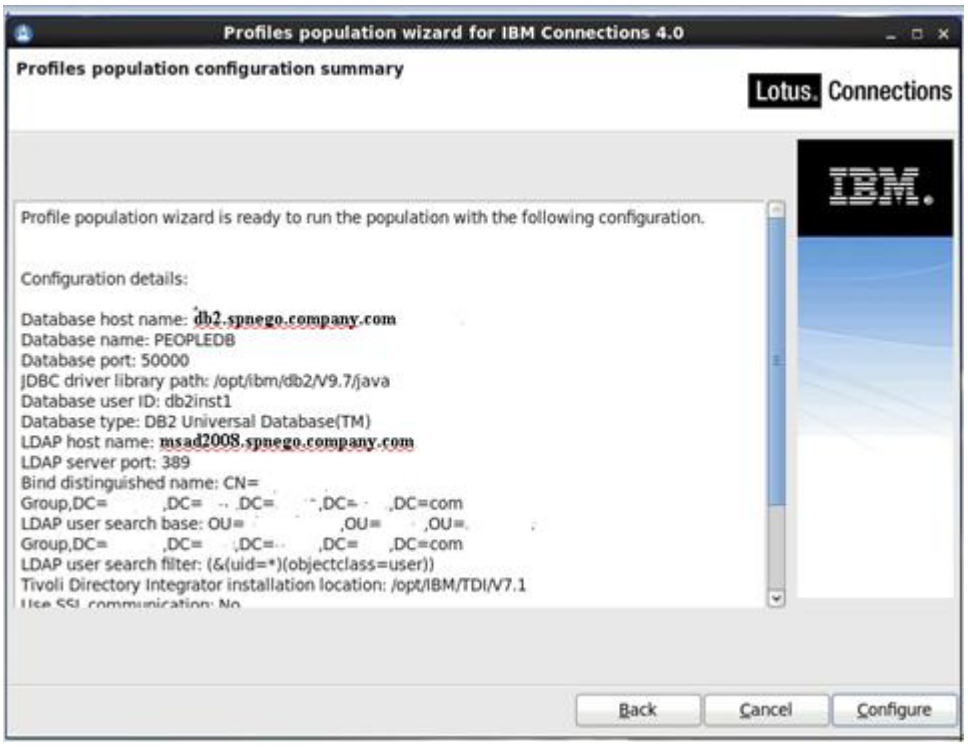


Figure 126. Profiles population wizard for IBM Connections 4.0: Profiles population configuration summary

The next screen indicates that the execution of the population task is in progress.

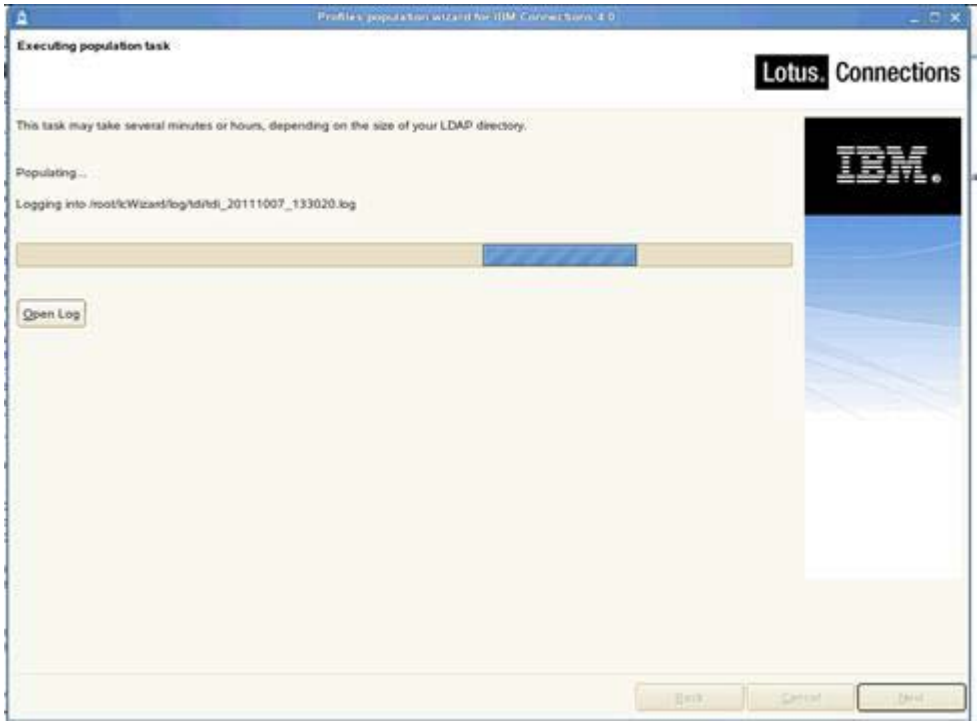


Figure 127. Profiles population wizard for IBM Connections 4.0: Executing population task

__ 15. When it finishes, you should see the following screen. Click **Finish** to exit the wizard.

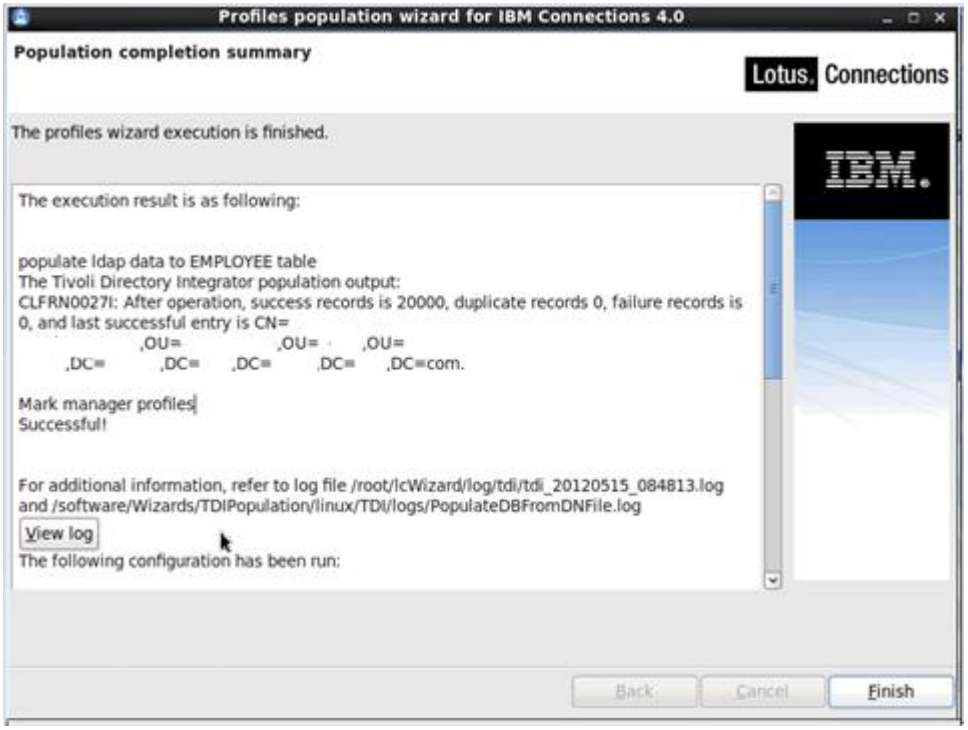


Figure 128. Profiles population wizard for IBM Connections 4.0: Population completion summary

Note

This task can take quite a long time depending on the number of users to populate.

Manual population of Profiles

Note

In this deployment there were almost 400,000 users in the LDAP that had to be populated to the `PROFILES` database. However, the `./populationWizard.sh` stopped after populating just the first 20k users. To get around this limitation we had to run the following manual steps to fully populate `PROFILES` with all 400k users from the LDAP.

__ 1. Make the following changes (in bold) to the Tivoli Directory Integrator file `ibmdisrv`:

__ 2. "$TDI_JAVA_PROGRAM" -Xms**256**M -Xmx**3072**M $TDI_MIXEDMODE_FLAG -Xnojit -cp "$TDI_HOME_DIR/IDILoader.jar".

__ 3. In the file `profiles_tdi.properties` (`.../lcWizard/log/tdi/`) update the entry `source_ldap_page_size` to a value of `1000`.

__ 4. Run the following command from the directory: `.../lcWizard/log/tdi/ ./collect_dns.sh`.

Note

This process takes several hours to complete.

__ 5. Make a backup copy of the file `collect.dns`, i. e. `cp collect.dns backup-collect.dns`.

__ 6. Split the file `collect.dns` into chunks of 20k users by running:

split -l 20000 collect.dns collect-split

Enter **ls -la collect-split*** and you can see the list of files created each with 20k users; in this case the following files were created:

```
collect-splitaa collect-splitab collect-splitac collect-splitad
collect-splitae collect-splitaf collect-splitag collect-splitah
collect-splitai collect-splitaj collect-splitak collect-splital
collect-splitam collect-splitan collect-splitao collect-splitap
collect-splitaq collect-splitar collect-splitas collect-splitat
```

__ 7. Populated the `PROFILES` database by running the following command**:**

```
for i in collect-splitaa collect-splitab collect-splitac collect-splitad
collect-splitae collect-splitaf collect-splitag collect-splitah
collect-splitai collect-splitaj collect-splitak collect-splital
collect-splitam collect-splitan collect-splitao collect-splitap
collect-splitaq collect-splitar collect-splitas collect-splitat ; do cp $i
collect.dns; ./populate_from_dn_file.sh $i ; rm -rf collect.dns; done
```

Note

This process took over 24 hours to run to completion and at the end the `PROFILES` database was populated with the 400k users.

6. Installation of IBM Connections v4.0

The installation of Lotus Connections 4.0 is done on the Deployment Manager computer and then synched with the nodes.

Requirements

Pre-requisites to install IBM Connection v4.0:

- In the Deployment Manager, verify that a user from the Deployment Manager's LDAP is granted administrator's access to the Deployment Manager.
- Make sure that your Deployment Manager is started and on each node, stop all running instances of WebSphere Application Server and WebSphere node agents.
- You must have created the Connections databases.
- If you are installing the Metrics application, ensure that you installed and configured Cognos.
- Ensure that the directory paths that you enter contain no spaces.
- Ensure that the Open File Descriptor limit is 8192 (see previously).
- Create a shared `location/folder` on the Deployment Manager computer and give all Node computers full read/write access to this share. (see previously).
- Copy the Connections build (`Lotus_Connections_4.0_lin_aix.tar` file) to the Deployment Manager computer and extract its contents.

__ 1. In the folder `IBM_Connections_Install`, start the installation by running `./launchpad.sh`. The IBM Connections 4.0.0 installation assistant displays. In the left pane, click **Install IBM Connections 4.0**.

Figure 129. IBM Connections 4.0.0: Welcome

__ 2. In the right pane, click **Launch the IBM Connections 4.0.0 install wizard**.

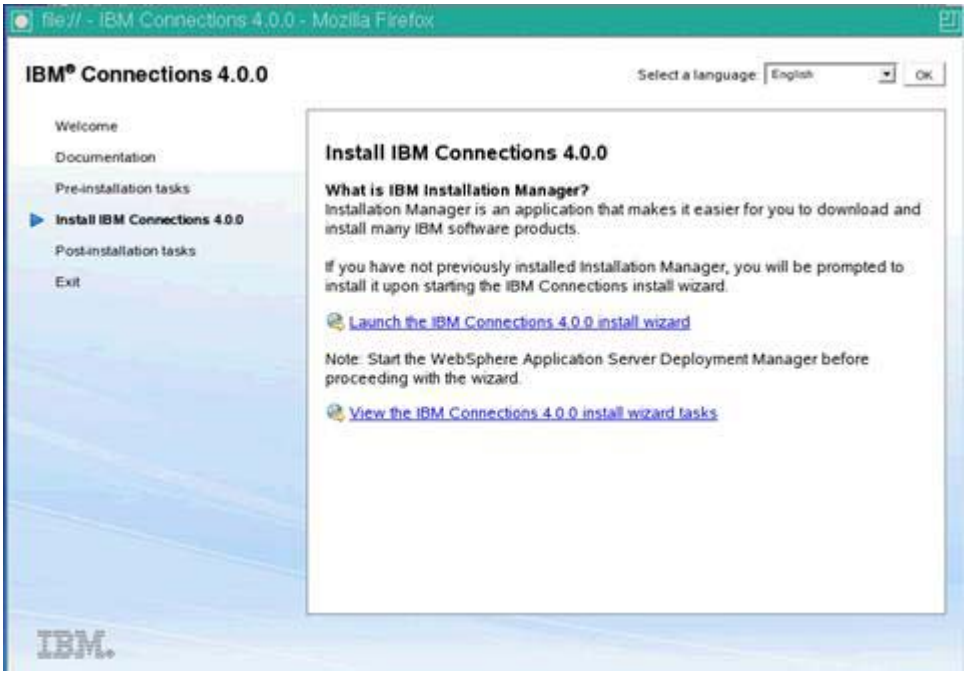


Figure 130. Installing IBM Connections 4.0.0

The following screen displays.

Figure 131. IBM Installation Manager

__ 3. Select the packages that you want to install. In this case, it is being installed on a system that did not have any previous installs. Selected all options and then click **Next**.

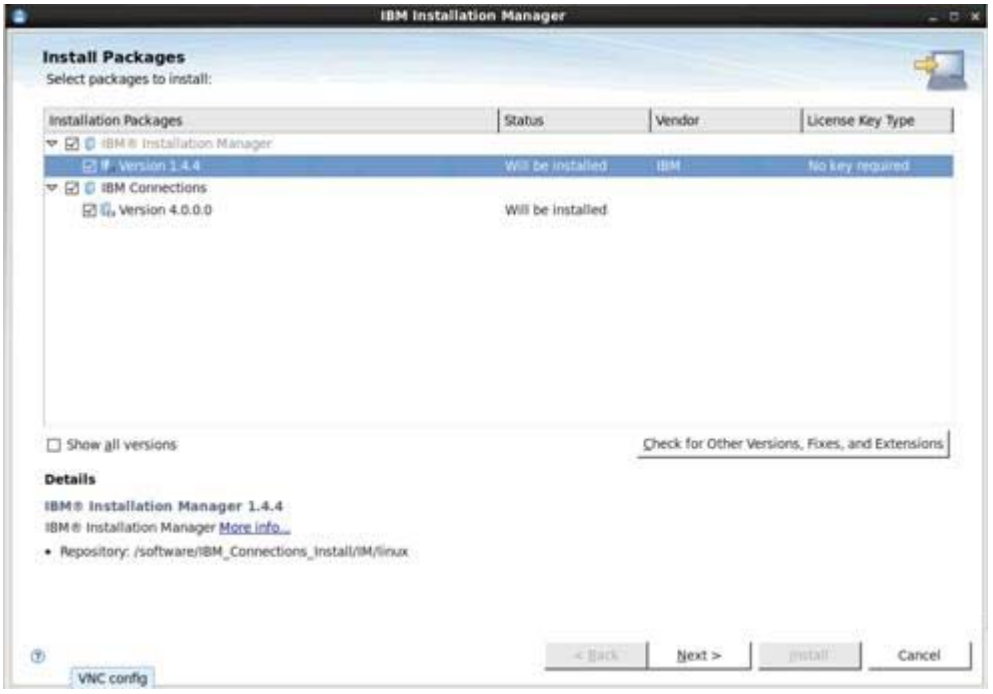


Figure 132. IBM Installation Manager: Selecting packages to install

__ 4. Review and accept the license agreement by clicking **I accept the terms in the license agreements**. Click **Next**.

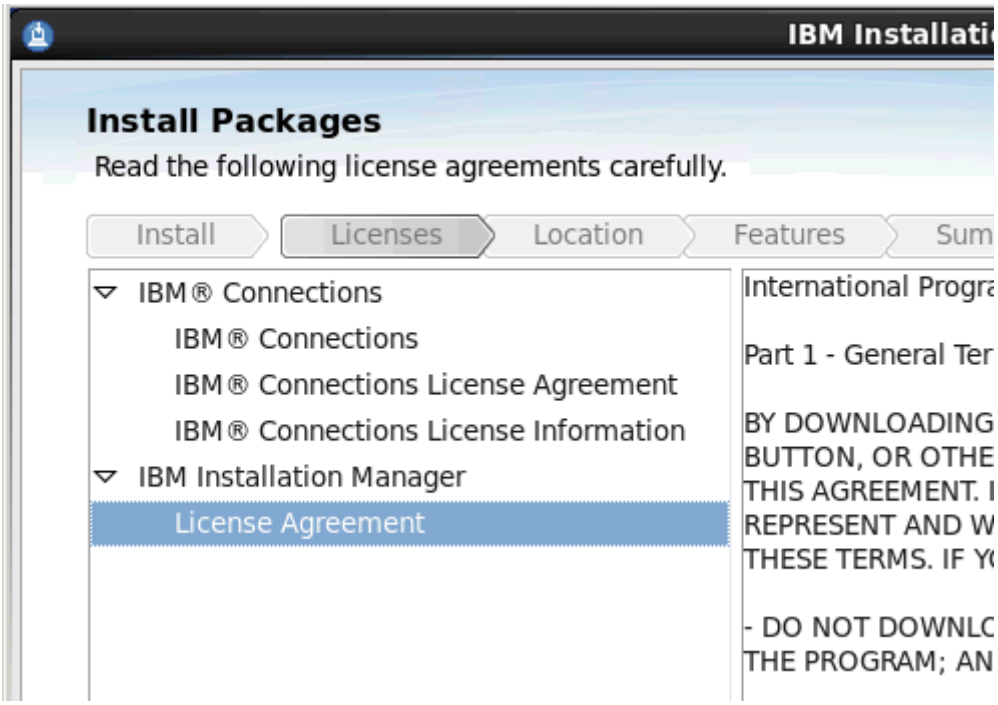


Figure 133. IBM Installation Manager: License agreements

__ 5. Specify the location of shared directories for IBM Installation Manager (you can use the default) and click **Next** to continue.

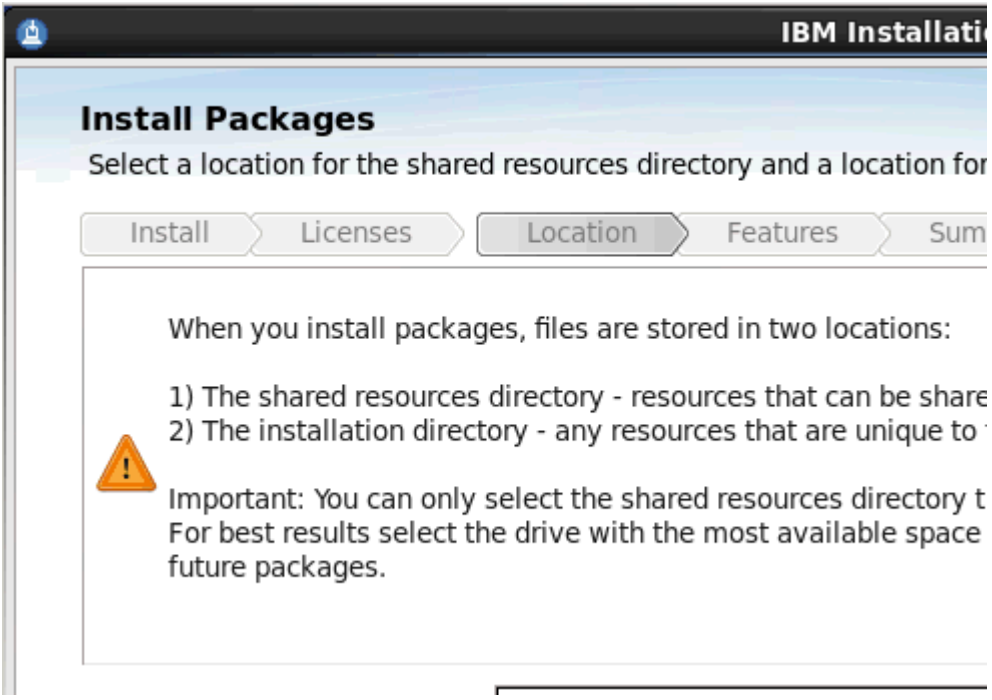


Figure 134. IBM Installation Manager: Location for the shared resources directory

__ 6. Choose to use the existing package group or create a package group.

Note

If this is the first time that you use the wizard, the “Use the existing package group” option is not available.

__ 7. Specify the location of the Installation Directory for IBM Connections. You can accept the default directory location. Enter a new directory name, or click **Browse** to select an existing directory. Then, click **Next** to continue.

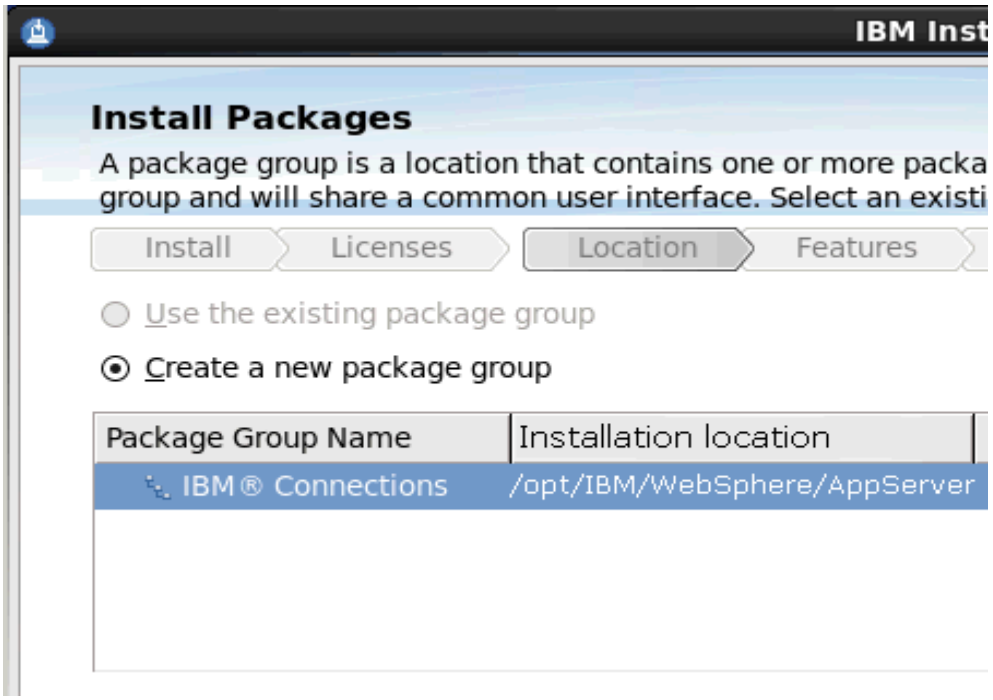


Figure 135. IBM Installation Manager: Package group

__ 8. Select the applications that you want to install and click **Next** to continue.

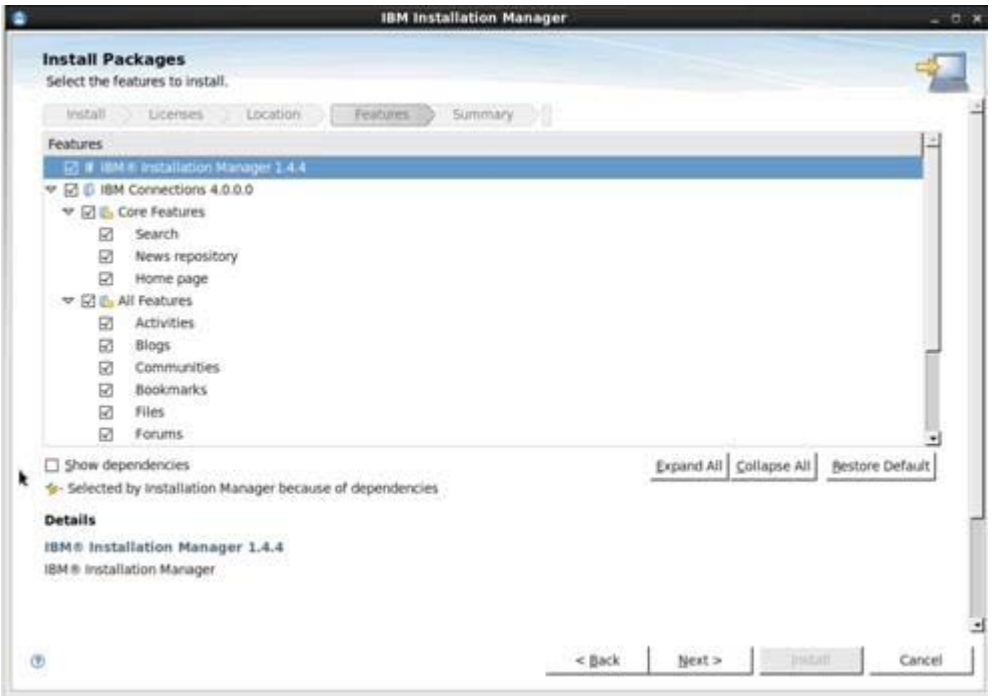


Figure 136. IBM Installation Manager: Features to install

__ 9. Enter the WAS Installation location; enter the host name, administrator user ID, and password. Then, click **Validate** at the bottom8.

Hint

Use an Administrator user ID that is from the LDAP (below that user is called `AdminUserFromLDAP`) and is configured as an Administrator on the WebSphere Application Server.

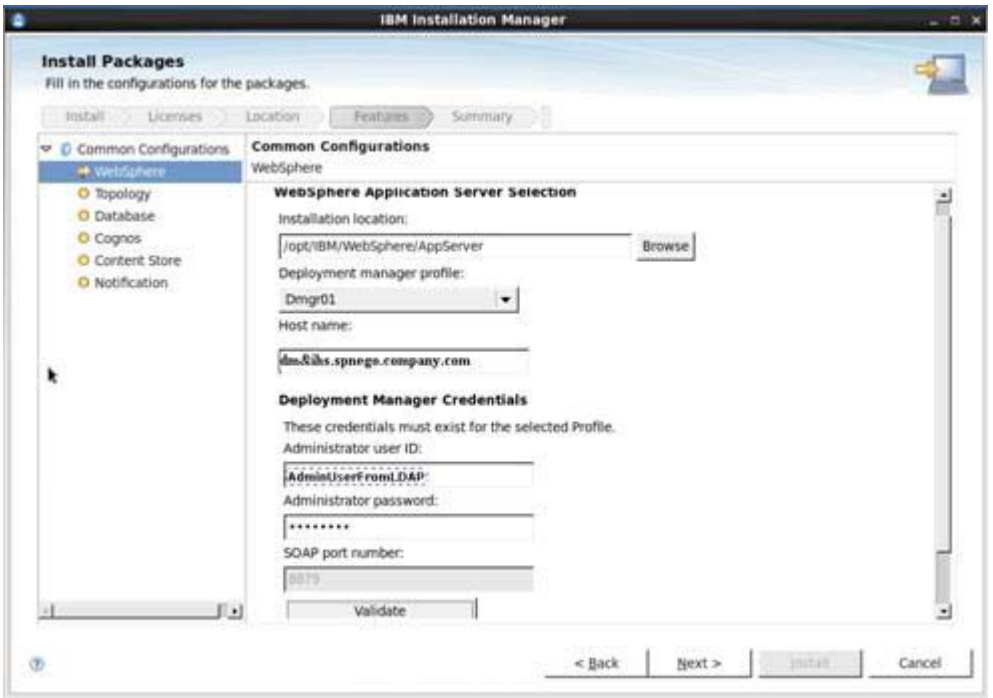


Figure 137. IBM Installation Manager: Configuration for the packages

The validation screen retrieves the SSL certificate from the Deployment Manager.

Figure 138. Checking application security

__ 10. After a few moments you should see the following message. Click **OK** to continue.

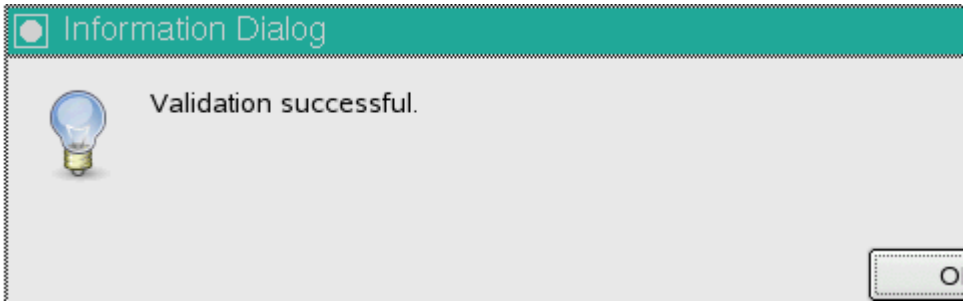


Figure 139. Information dialog: Validation successful

__ 11. Select the Deployment topology. Click **Medium: Applications grouped in several clusters**.

__ 12. Select the nodes on which you want to create the Applications/Clusters.

__ 13. Click **Next** to continue.

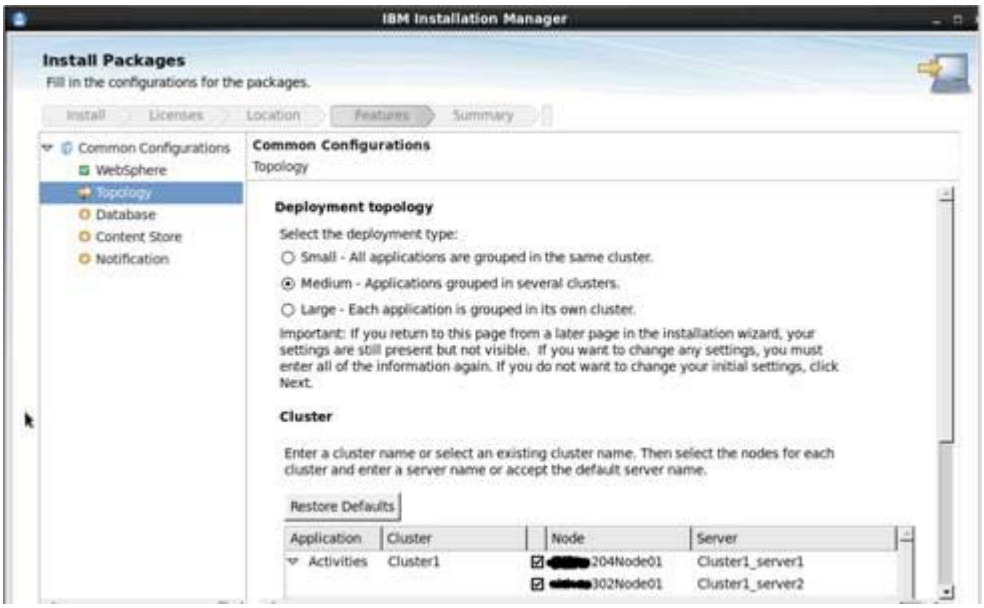


Figure 140. Deployment topology (1 of 3)

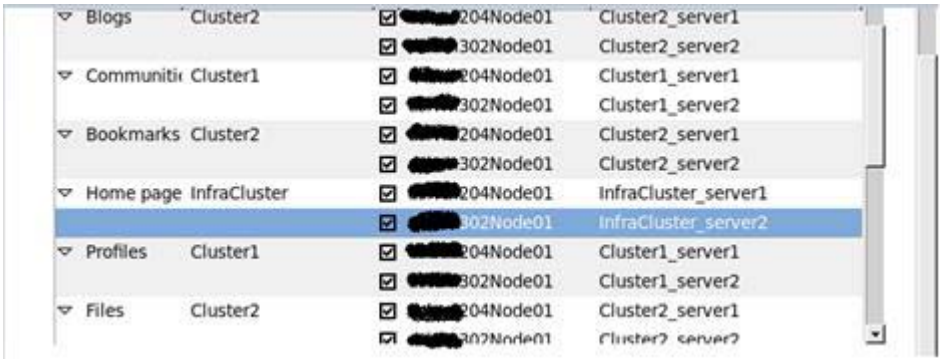


Figure 141. Deployment topology (2 of 3)

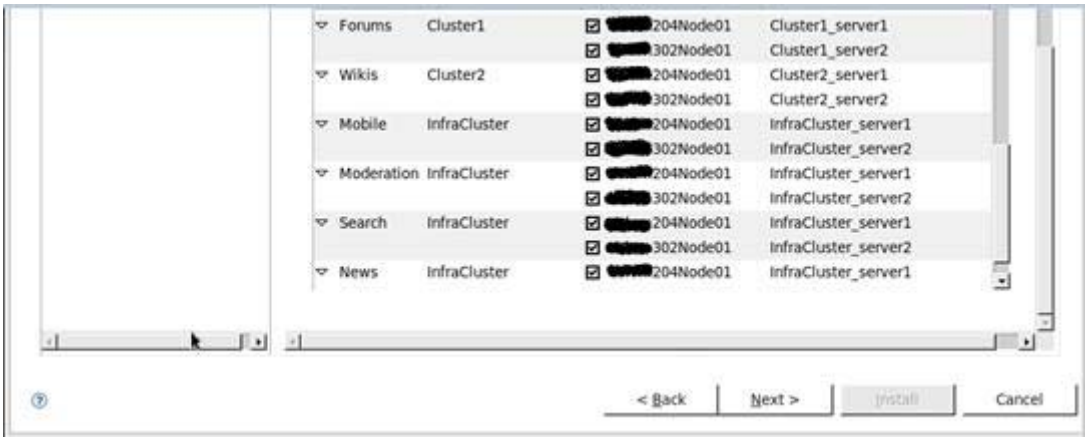


Figure 142. Deployment topology (3 of 3)

__ 14. Next, you configure the database. Ensure that your database server is started.

__ 15. Select **Yes, the applications are on the same database instance**.

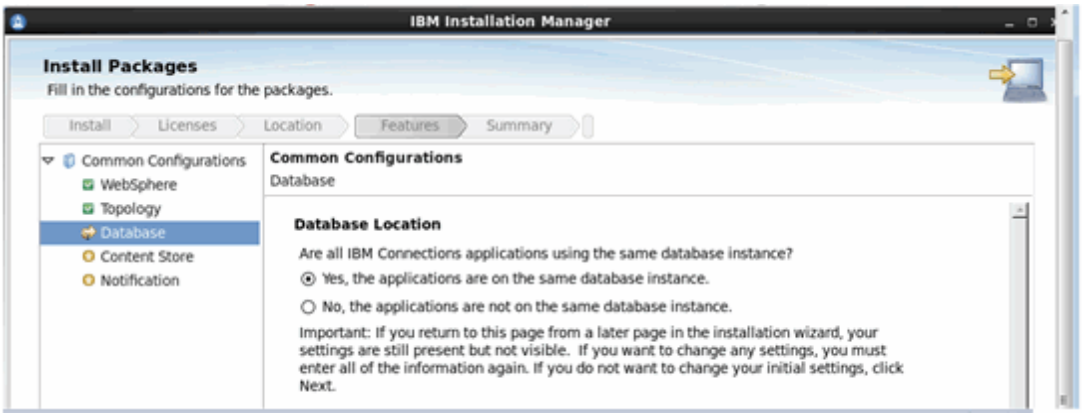


Figure 143. IBM Installation Manager: Completing the configurations for the packages

__ 16. Enter the database server details (host name and port) of your database server.

Figure 144. IBM Installation Manager: Database server information

__ 17. Enter the JDBC driver location.

__ 18. Enter the users and passwords that you created the databases with. Click Validate at the bottom of the panel.

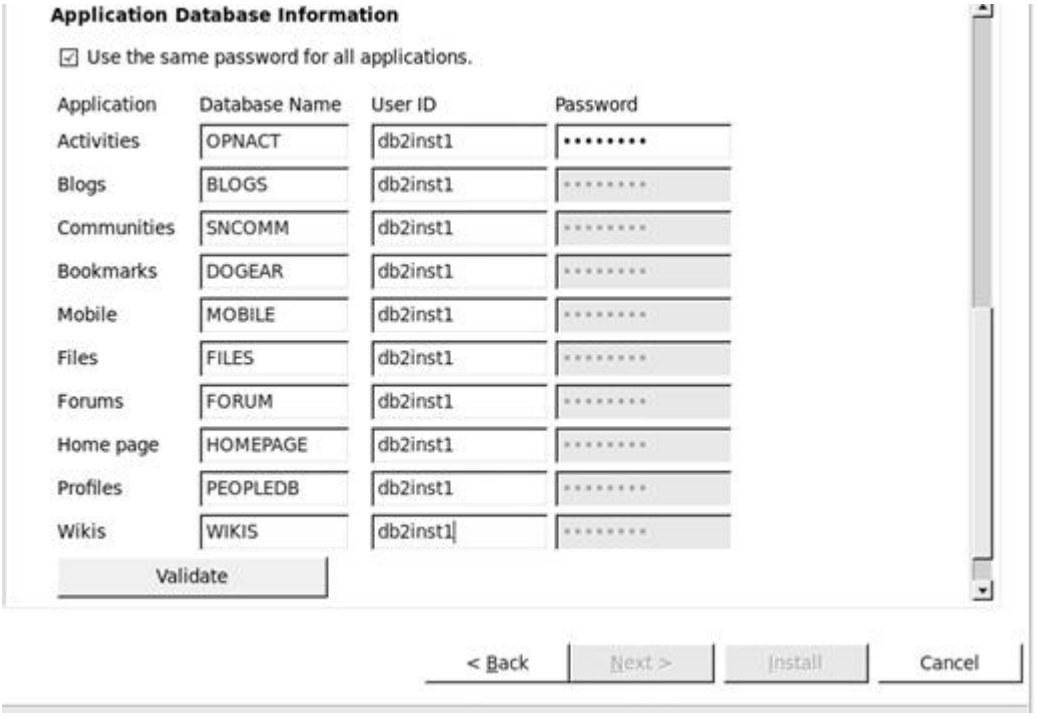


Figure 145. IBM Installation Manager: Application database information

The following message is displayed.

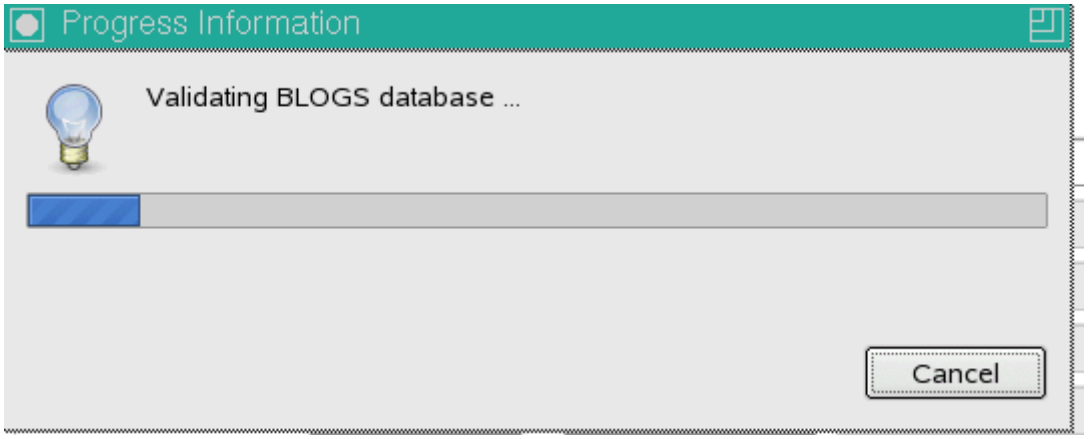


Figure 146. Progress Information: Validating BLOGS database

__ 19. When the validation completes, click **OK** to continue.

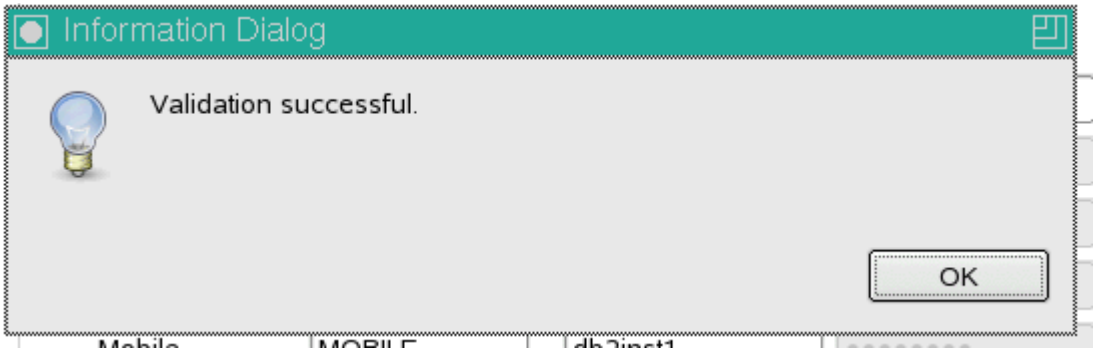


Figure 147. Information dialog: Validation successful

__ 20. Next, configure **Content Store**.

As the Deployment Manager and Nodes are installed on different computers, a common share location is configured on the Deployment Manager system that is shared with each of the nodes.

Specify this shared location in the "Select a network shared location". In this case, it is called `/opt/IC_Share`.

The click **Validate**.

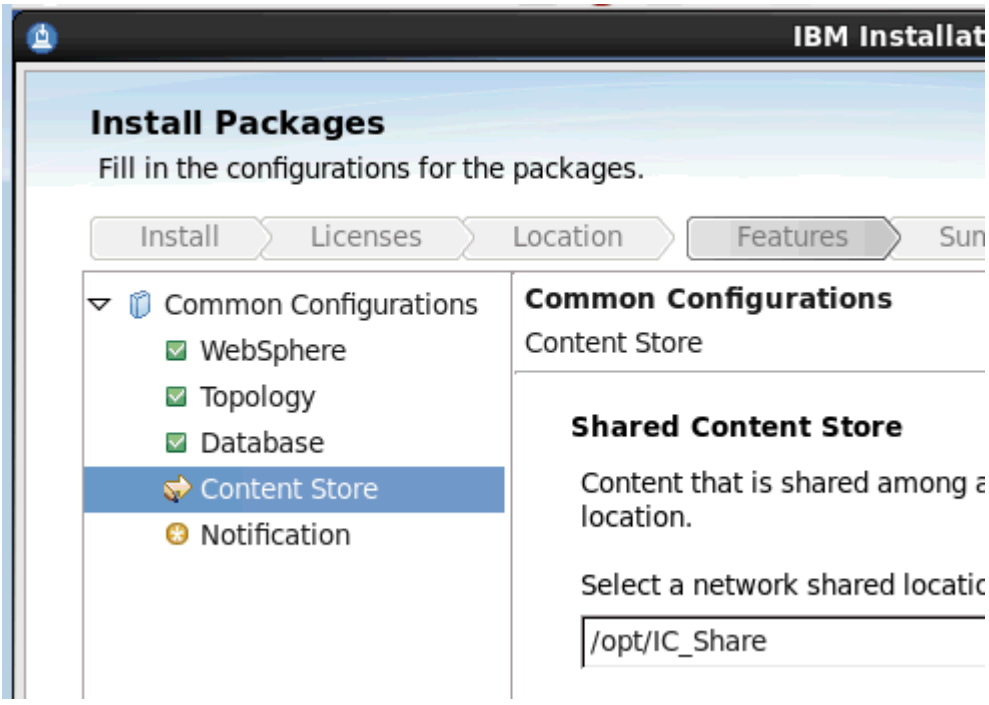


Figure 148. Configuring Content Store

__ 21. When the validation completes, click **OK** and then **Next**.

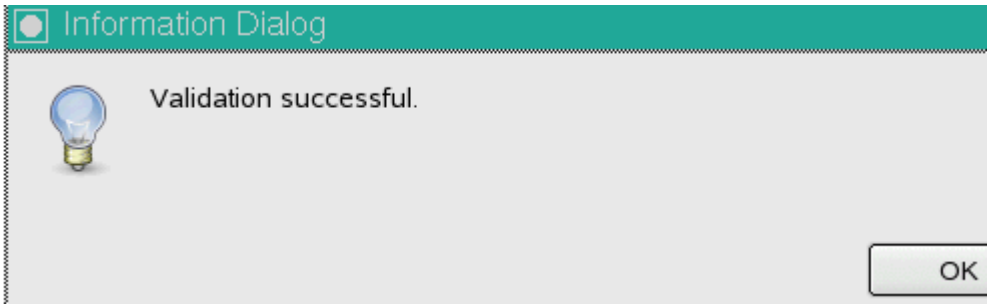


Figure 149. Information dialog: Validation successful

__ 22. Finally, in the Notification screen select **None** (Notification will be enabled at a later stage).

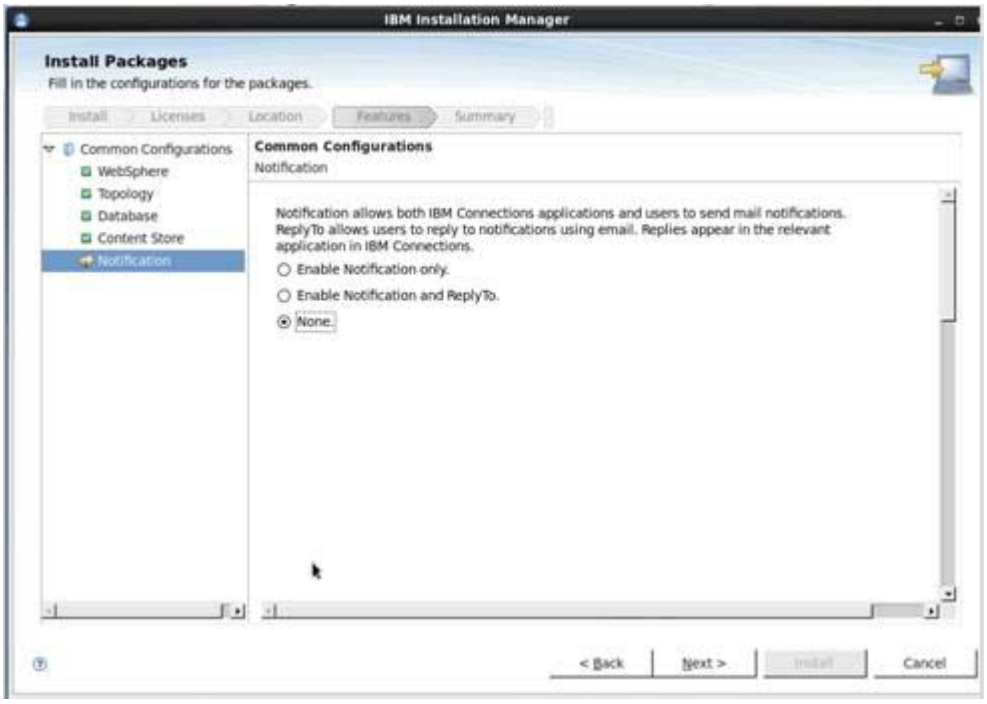


Figure 150. Configuration for the packages: Notification

__ 23. Finally, the summary screen displays. After you verified the details, click **Install**.

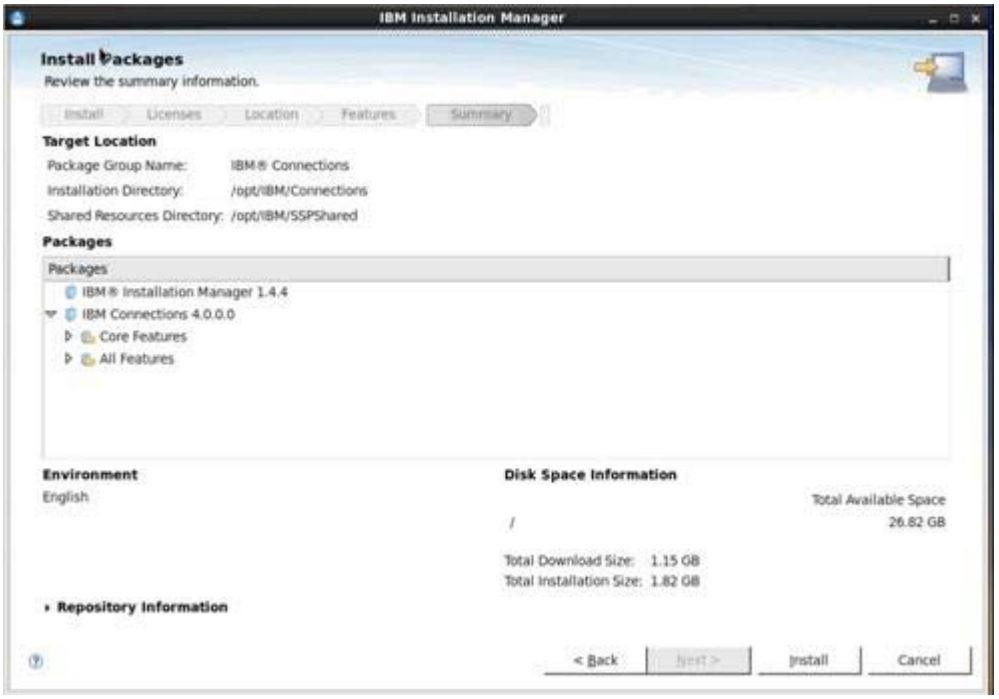


Figure 151. IBM Installation Manager: Summary information

The installation starts. You see an Installing dialog like in the following figure.

Figure 152. Installing information

When the installation completes, you should see the following figure:

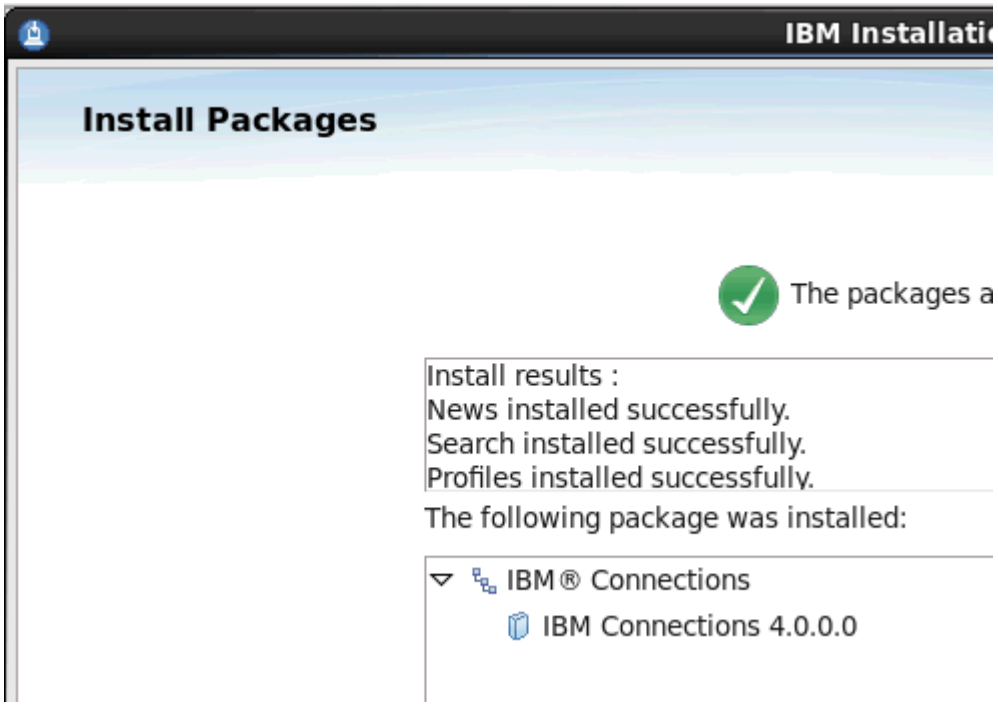


Figure 153. IBM Installation Manager: installation results

__ 24. Review the result of the installation. Click **Finish** to exit the installation wizard.

__ 25. Next, deploy the IBM Connection Applications to each node. Stop and restart the Deployment Manager (Deployment Manager) as follows:

__ a. Open a command prompt.

__ b. Change to the directory: `cd /opt/WebSphere/AppServer/bin`.

__ c. Stop the Deployment Manager by entering the `./stopManager.sh` command.

__ d. When the Deployment Manager stopped, restart it by entering the `./startManager.sh` command.

__ 26. Start the node agents on each node and perform a Full Resynchronize:

__ a. On each node system, start the node agent by entering the `./startNode` command.

```
:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin # ./startNode.sh
ADMU0116I: Tool information is being logged in file
           /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/nodeagent/startServer.log
ADMU0128I: Starting tool with the AppSrv01 profile
ADMU3100I: Reading configuration for server: nodeagent
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server nodeagent open for e-business; process id is 8350
dslvm1008:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin #
```

Figure 154. ./startNode command

__ b. Log in to the **Integrated Solutions Console** on the Deployment Manager to fully resynchronize all nodes.

i. Go to **System administration** > **Nodes**.

ii. Select the nodes and click **Full Resynchronize**.

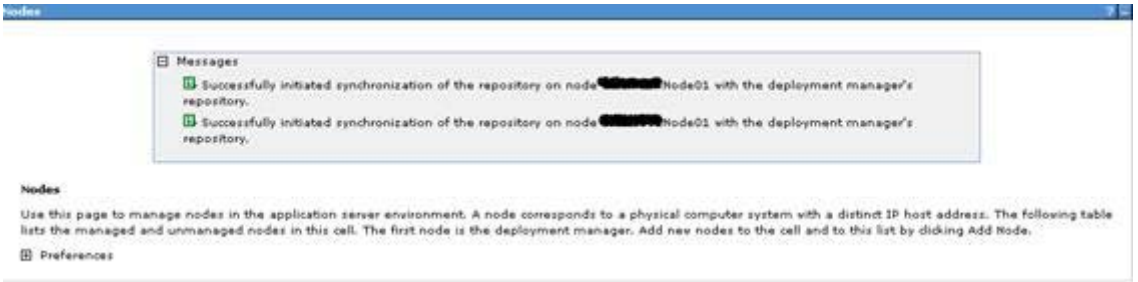


Figure 155. Full resynchronize

You can also check the logs on both Node 1 and Node 2 for successful synchronization. You should see the following messages:

```
[redacted]:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/nodeagent # ls
SystemErr.log  SystemOut.log  SystemOut_11.10.11_13.56.25.log  monitor.state  native_stderr.log  native_stdout.log  nodeagent.pid  startServer.log
[redacted]/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/nodeagent # tail -f SystemOut.log
[10/19/11 16:41:27:580 IST] 00000034 NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
[10/19/11 16:42:27:592 IST] 00000035 NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
[10/19/11 16:43:05:819 IST] 0000000d FileRepositor A   ADMR0012I: The repository epoch is refreshed.
[10/19/11 16:43:34:769 IST] 00000036 NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
[10/19/11 16:44:27:600 IST] 00000037 NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
[10/19/11 16:45:27:614 IST] 00000038 NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
[10/19/11 16:46:27:622 IST] 00000039 NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
[10/19/11 16:47:27:618 IST] 0000003a NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
[10/19/11 16:48:27:631 IST] 0000003b NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
[10/19/11 16:49:27:637 IST] 0000003c NodeSyncTask  A   ADMS0003I: The configuration synchronization completed successfully.
```

Figure 156. Successful synchronization messages

Note

Wait until the Deployment Manager copies all the application EAR files to the installedApps directory on each of the nodes. This process can take up to 30 minutes. To find out whether the process is complete, log in to each node and go to the installedApps directory and ensure that all the application EAR files are fully extracted.

The default path for where the applications are copied to is:

`/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/`.

Figure 157. Default path where applications are copied

__ 27. Restart the Deployment Manager.

__ 28. Start all your IBM Connections clusters:

__ a. Log in to the Integrated Solutions Console on the Deployment Manager.

__ b. Go to **Servers** > **Clusters** > **WebSphere Application Server clusters**.

__ c. Select the IBM Connections clusters and click **Start**.

Note

It takes several minutes for all clusters to start.

7. Post-IBM Connections installation steps

Configure notifications

Computer host name	Applications	Version#	OS/version	RAM / CPU	VM or HW
dm&ihs.spnego.company.com	WebSphere Application Server Deployment Manager IBM HTTP Server	WebSphere Application Server v7.0.0.21 (64 bit) IBM HTTP Server v7.0.0.21	RedHat 6 (64 bit)	8G / 2CPUs	VM
domino.company.com	Domino Mail-in server	Domino 8.5.3	Win2008 R2 EE Server	4G / 2CPUs	VM

Configuring Notifications involves the following steps:

- Create a special ReplyTo user on the Domino mail server
- Configure the ReplyTo user in Domino
- Configuring Domino for email notification replies
- Configuring WebSphere Application Server Deployment Manager for email notification replies
- Enabling notification replies in IBM Connections
- Troubleshooting

Create a special ReplyTo user on the Domino mail server

__ 1. Open the Domino Admin client, and connect to Domino mail server.

__ 2. Select **People & Group** view and then click the **People** tab on the right panel.

__ 3. Click **Register** and input the certifier's password for the Domino server.

__ 4. Check the **Advanced** box and create a **ReplyTo** user as follows:

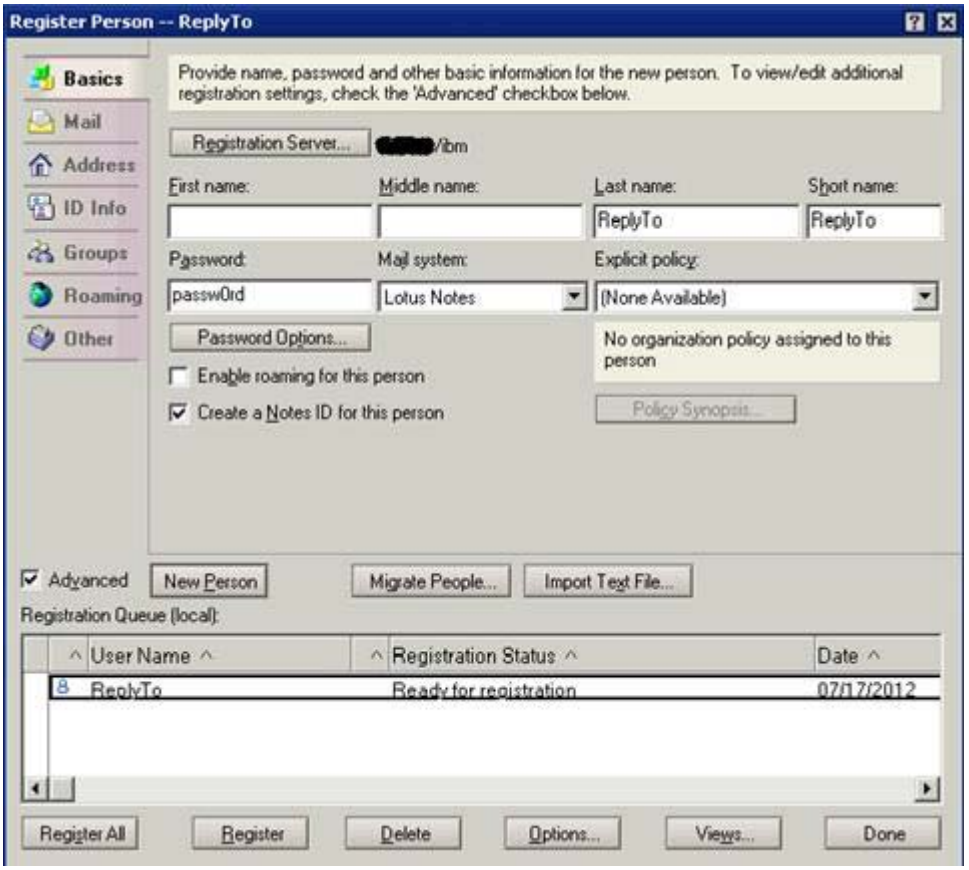


Figure 158. Register Person: ReplyTo

__ 5. The **Internet Domain** value might be set to the real domain you use.

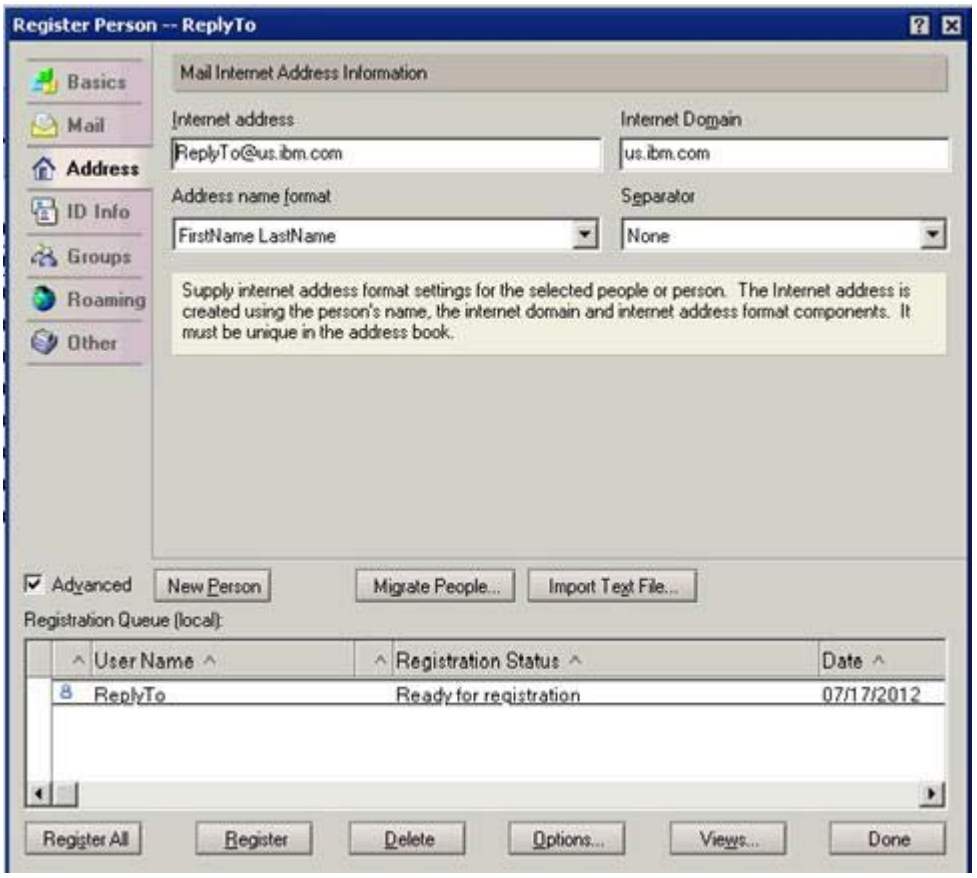


Figure 159. Internet Domain

__ 6. Click **Register** to complete the registration.

Configure the ReplyTo user in Domino

__ 1. Go back to **People & Groups** tab and expand **People by Organization**. Edit the account of the user that is used to direct reply mail (the **ReplyTo** user).

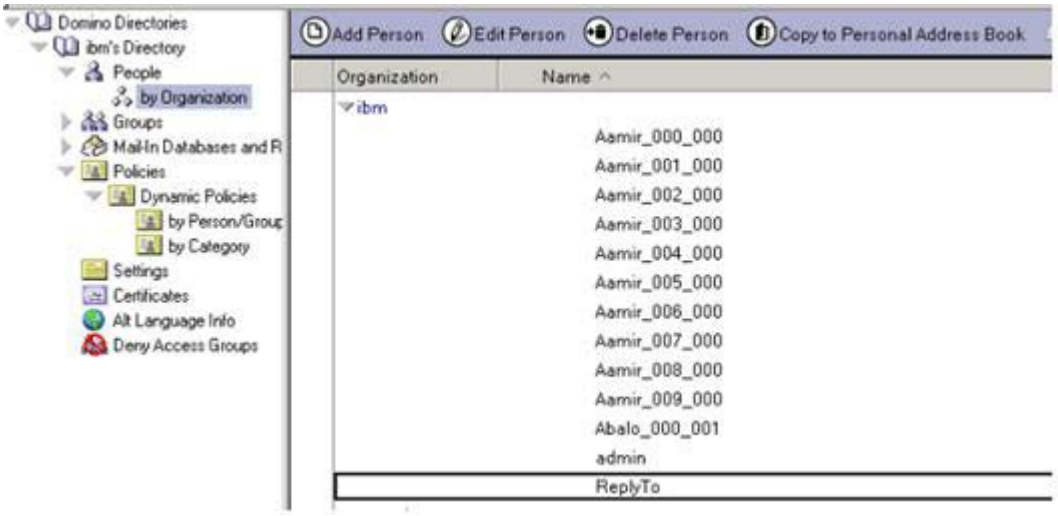


Figure 160. People & Groups > People by Organization

__ 2. Click **Open Mail File** for the ReplyTo user.

__ 3. Click **View > Agents**.

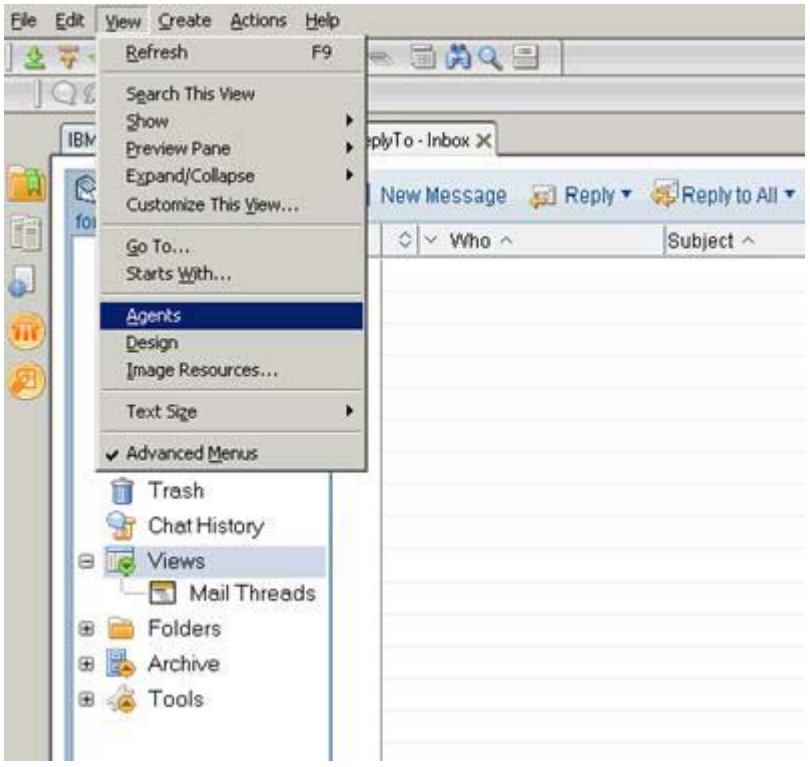


Figure 161. View: Agents

__ 4. Click **New Agent**.

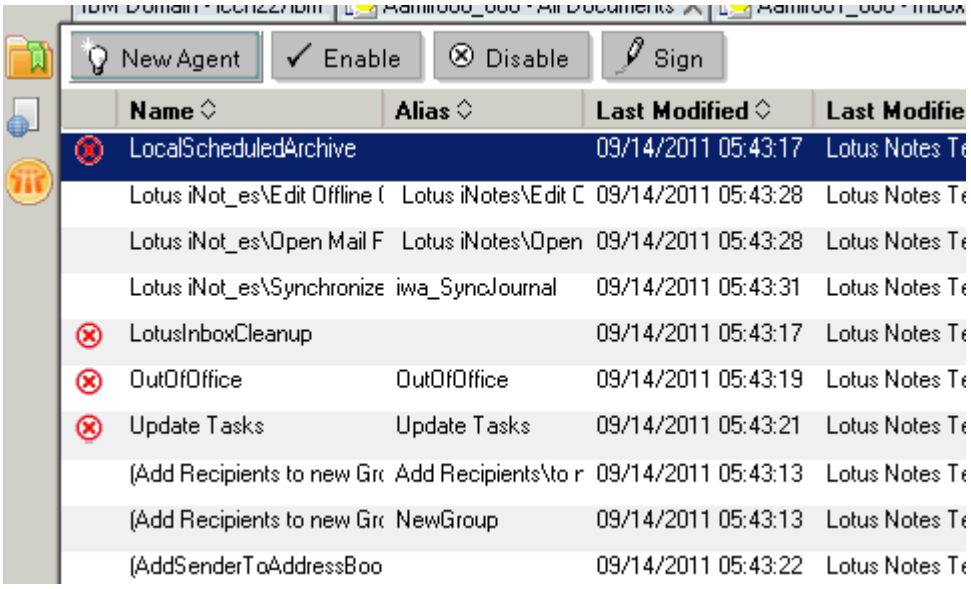


Figure 162. New Agent

__ 5. Set the Name field to `replyto`.

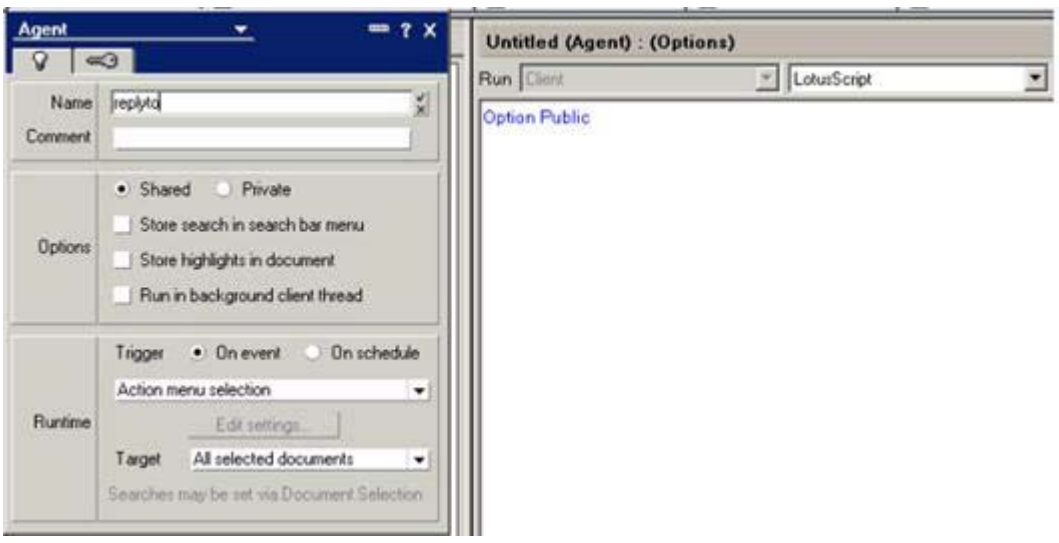


Figure 163. Setting the Name field

__ 6. Add the following LotusScript code to the agent:

```
Sub Initialize
   Dim session As New NotesSession
   Dim db As NotesDatabase
   Dim view As NotesView
   Dim doc As NotesDocument
   Set db = session.CurrentDatabase
   Set view = db.getView("$Sent")
   Set doc = view.GetFirstDocument()
   While Not(doc Is Nothing)
      Call doc.PutInFolder("$inbox")
      Set doc = view.GetNextDocument(doc)
   Wend
End Sub
```

Figure 164. Adding LotusScript code to the agent

__ 7. Click **Yes** to save your changes.

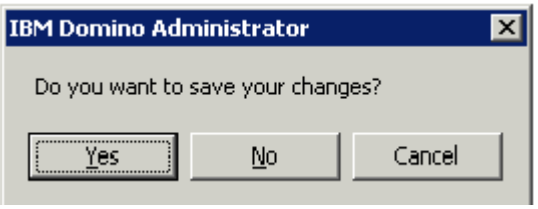


Figure 165. IBM Domino Administrator: Saving changes

__ 8. Open the agent again to set the following properties:

__ a. In the **Options** section, select **Shared**.

__ b. In the **Runtime** section, select **On schedule**, and then select **More than once a day**.

__ c. In the **Target** field, select **All new & modified documents**.

__ d. Click **Schedule** and set a schedule to run every 5 minutes, all day.

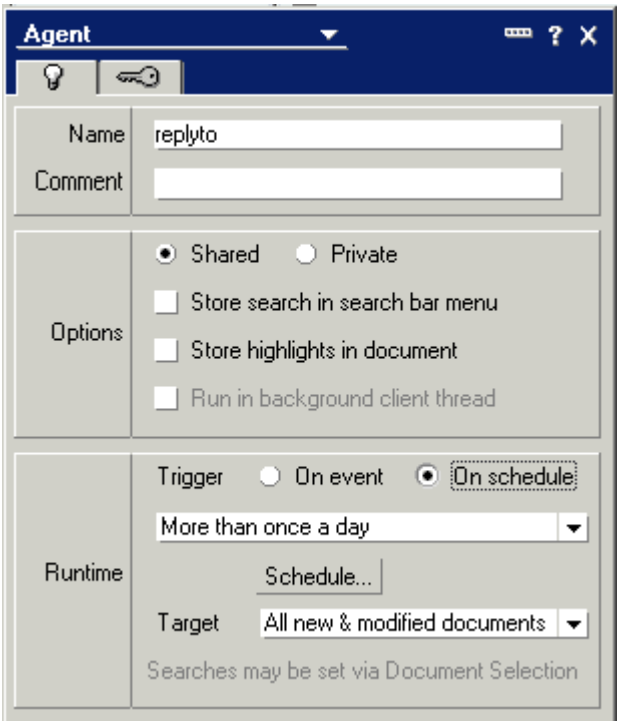


Figure 166. Agent properties

Configuring Domino for email notification replies

__ 1. Open Domino Admin client and click the **Configuration** tab.

__ 2. Expand **Messaging** in the navigator panel, and then click **Configuration**.

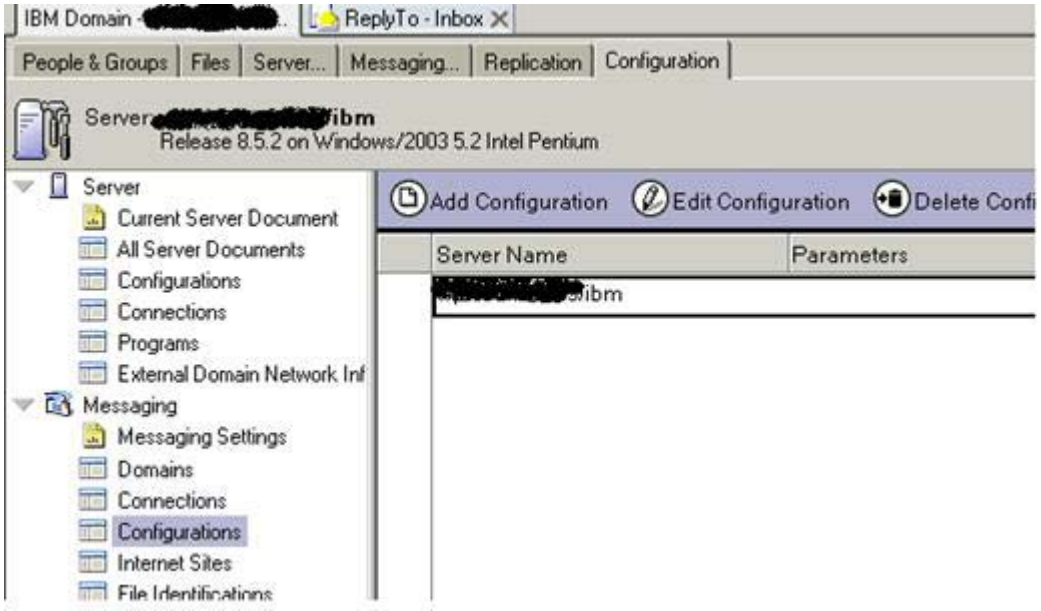


Figure 167. Configuring Domino for email notification replies

__ 3. Select the messaging server record and click **Edit Configuration**.

__ 4. Click the **Router/SMTP** tab, then the **Restrictions and Controls** tab, and then the **Rules** tab. Finally, click **New Rule**.

Figure 168. Router/SMTP > Restrictions and Controls tab > Rules tab

__ 5. Create a rule that moves emails that have the string `lcreplyto_` in the 'To' field to the mailbox as follows:

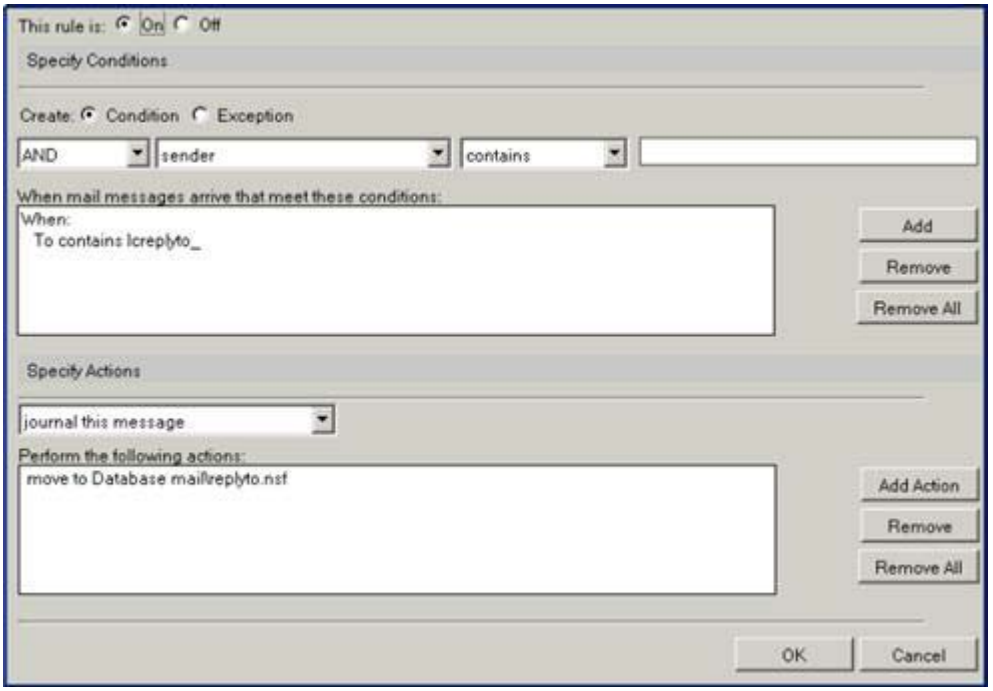


Figure 169. Creating a rule that moves emails that have the string `lcreplyto_` in the 'To' field

__ 6. Save and close.

__ 7. Stop and restart the Domino server

Configuring WebSphere Application Server Deployment Manager for email notification replies

__ 1. Log in to the WebSphere Application Server Console: `https://dm&ihs.spnego.company.com:9043/ibm/console`.

__ 2. Select **Resources > Mail > Mail Sessions > lcnotification > Custom properties**.

__ 3. Configuring the Mail Session `lcnotification`:

__ a. Create or edit the following general properties and outgoing mail properties:

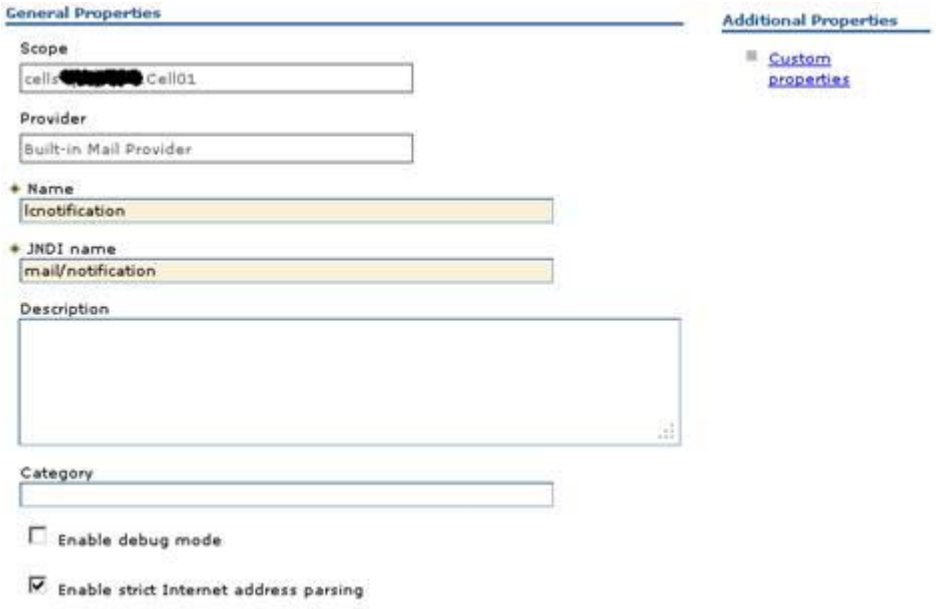


Figure 170. General Properties

Figure 171. Outgoing Mail Properties

__ b. Click **OK** and **Save**.

__ c. Go to **Mail Sessions > lcnotification > Custom properties**.

i. Create or verify the following settings:

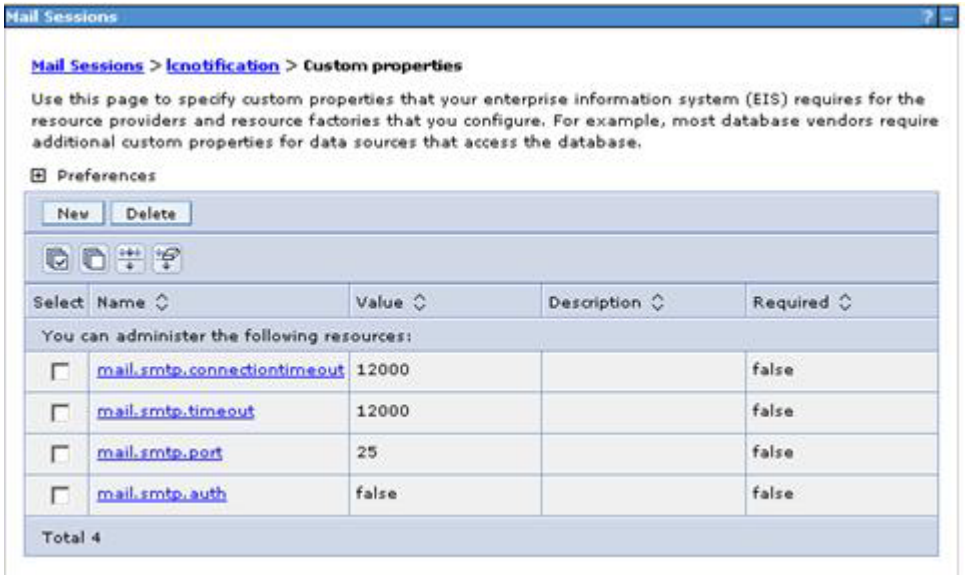


Figure 172. Mail Sessions > lcnotification > Custom properties

__ 4. Configuring the Mail Session `lcreplyto`:

__ a. Go to **Resources > Mail > Mail Sessions**.

i. Create/edit the mail session `lcreplyto` defining the general properties and incoming mail properties:

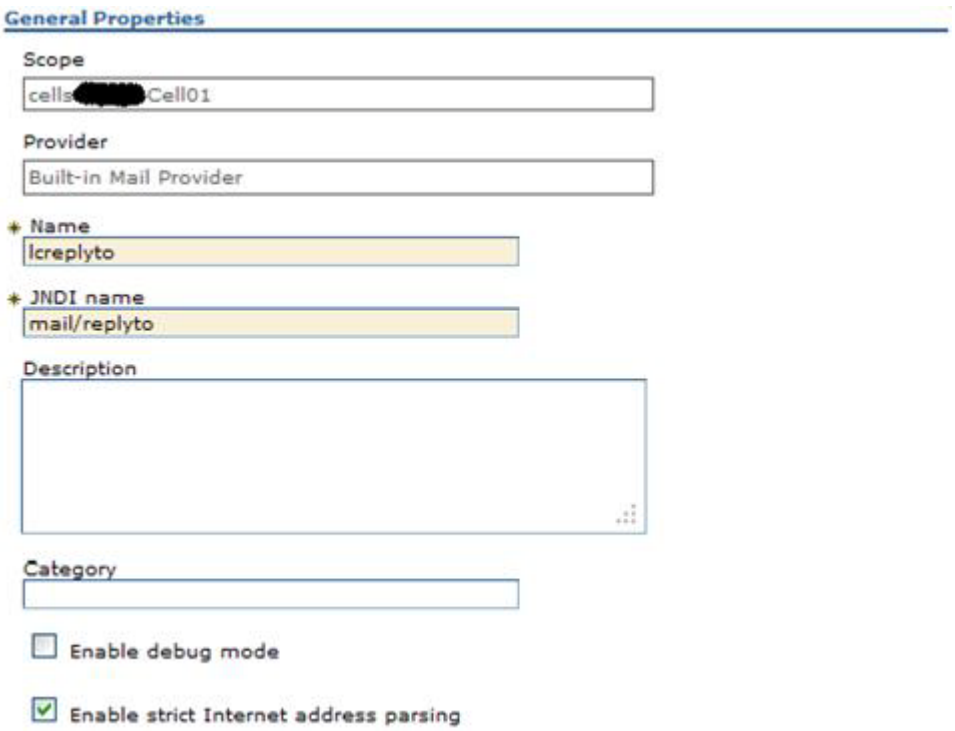


Figure 173. General properties

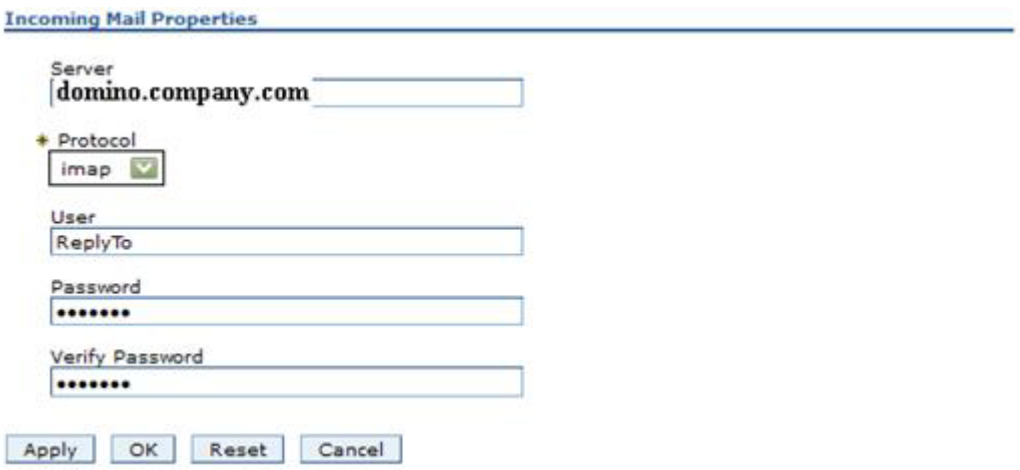


Figure 174. Incoming Mail Properties

i. Click **OK** and **Save**.

The final result should be as follows:

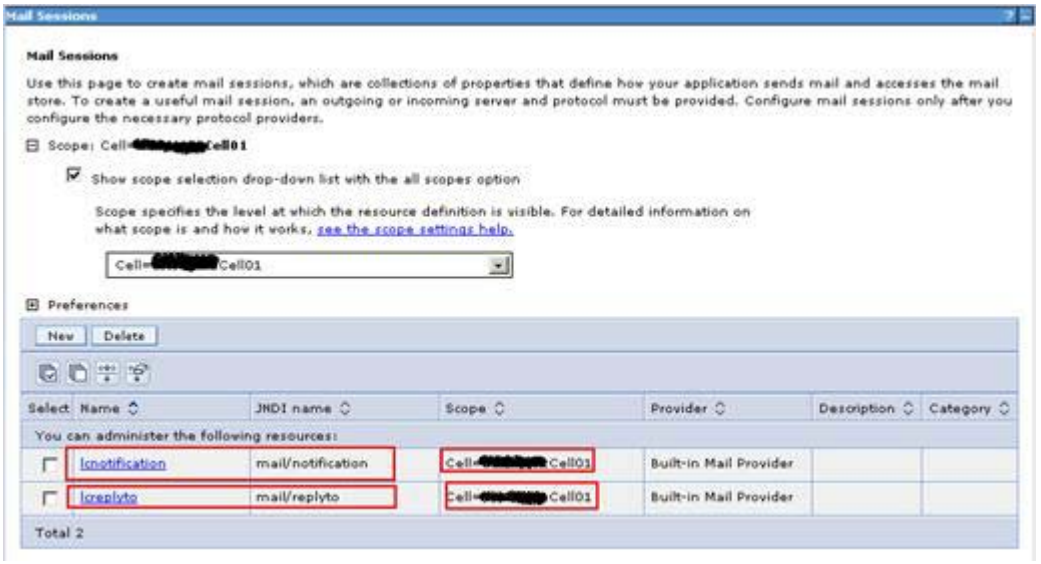


Figure 175. Mail sessions

Enabling notification replies in IBM Connections

__ 1. Using `wpadmin` checkout the file `news-config.xml`, open the file and search for the section "**mailin**" and make the following changes in bold: **_lcreplyto**

```
<mailin enabled="true">
<replyto enabled="true">

 <!-- A special ReplyTo address is added to notifications where
 the user can reply to the notification to respond/comment.
 The domain may be a dedicated domain for connections bound
 mails. Or it could be existing domain, in which case a prefix
 of suffix should be provided also. -->
   <replytoAddressFormat>
      <domain>us.ibm.com</domain>
      <!-- A prefix OR suffix (not both) may also be provided.
This is necessary if an existing domain (with other
email addresses) is being used.
There is a 28 character limit for the affix. -->
      <!--
      <affix type="suffix">_lcreplyto</affix>
      <affix type="prefix">lcreplyto_</affix>
      -->
<affix type="prefix">lcreplyto_</affix>
      </replytoAddressFormat>
   </replyto>
</mailin>
```

__ 2. Save the file and check it back in.

__ 3. Restart IBM Connections and the Deployment Manager.

   __ a. From the WebSphere Application Server console:

      i. Sync all nodes.

      ii. Stop all Connections Clusters.

   __ b. Stop and Restart the Deployment Manager.

   __ c. From the WebSphere Application Server console, start all Connections Clusters.

Troubleshooting

__ 1. If you encounter the following warning when you try to run the agent, then you must ensure that you have adequate permissions.

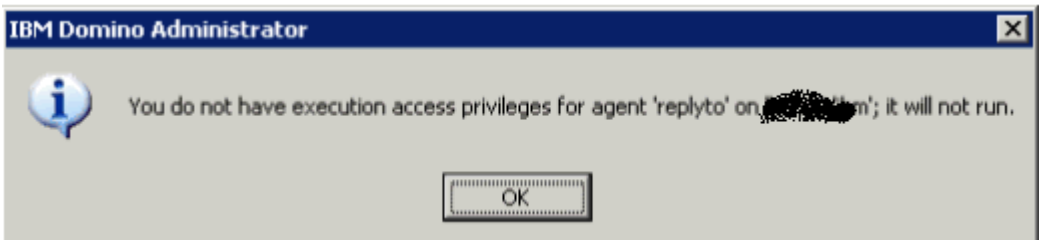


Figure 176. IBM Domino Administrator

__ 2. To fix the problem, open the server configuration from **Configuration > Server > All Server Documents** and edit it:

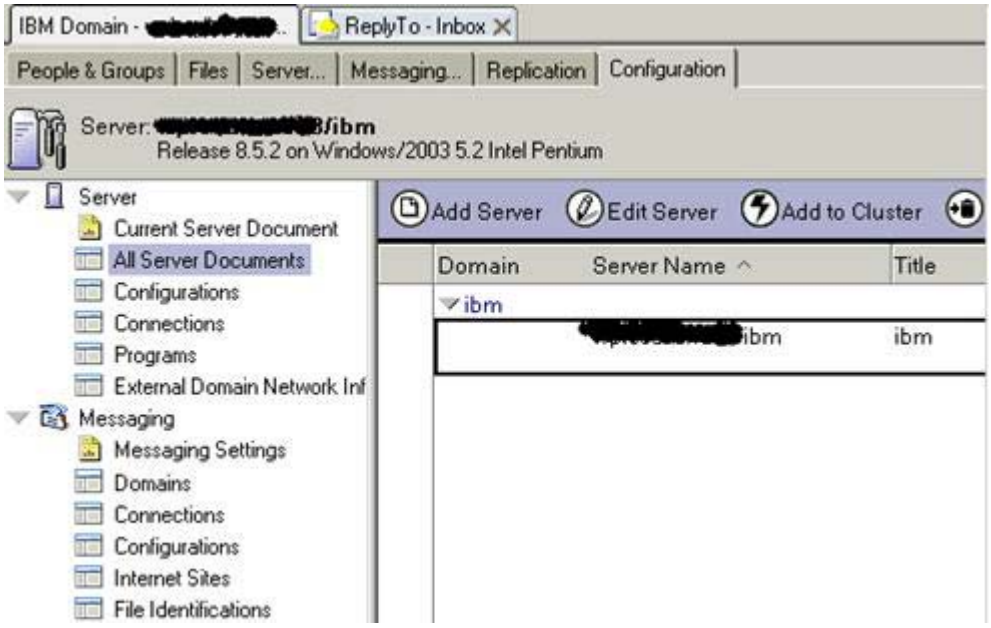


Figure 177. Editing the server configuration

__ 3. In the security tab, add administrator authorization for admin and the domino server as shown in the following figure.

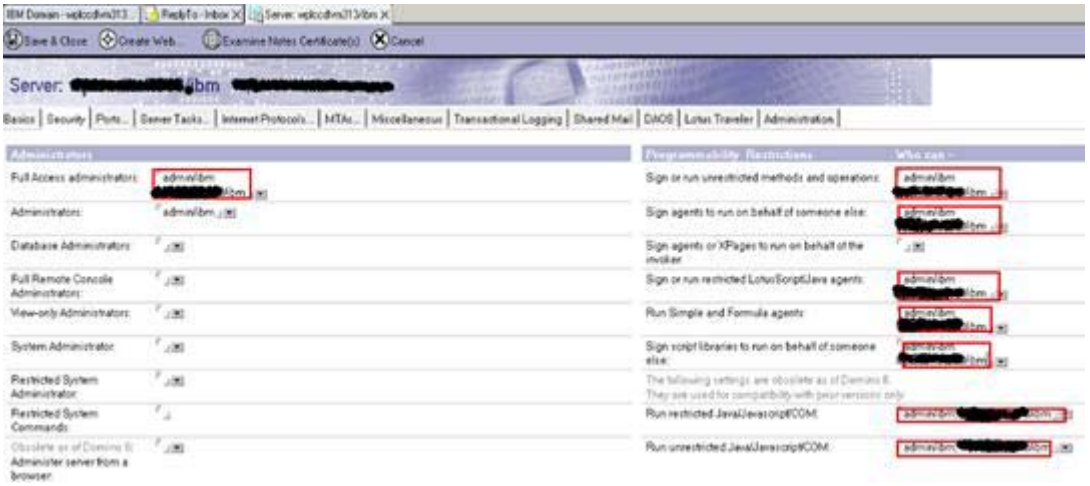


Figure 178. Adding an administrator authorization for admin and the domino server

Copy Search conversion tools (Stellent) to local nodes

Information

Visit `Copying Search conversion tools to local` nodes in the information center to get more information about this topic.

__ 1. For each Search server (i. e. node1 and node2), we copy the entire `Stellent` folder (which is located on the shared drive in the folder: `/opt/IC_Share/search/`), to the search folder on the local drive i. e. :

   __ a. Copy `/opt/IC_Share/search/stellent` (entire folder and sub-folders) to: `/opt/IBM/Connections/data/local/search` (local drive).

   __ b. Verify that the entire folder has been copied to the local drive.

__ 2. In the WebSphere Application Server console, set the variable `FILE_CONTENT_CONVERSION=/opt/IBM/Connections/data/local/search/stellent/dcs/oiexport/exporter`.

__ 3. Edit the file `setupCmdLine.sh` and add the following export statements:

   `vi /opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh`

   Add:

   `export PATH=$PATH:/opt/IBM/Connections/data/local/search/stellent/dcs/oiexport`

   `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/IBM/Connections/data/local/search/stellent/dcs/oiexport`.

__ 4. Also, add the previous export statements to the `/etc/profile` file.

Configuring the HTTP server

This section is about configuring the HTTP web server after installing IBM Connections.

__ 1. Before beginning this task, ensure that the IBM HTTP Administration server is started. The admin server must be started to synchronize configuration files between the HTTP Server and the Deployment Manager.

__ 2. Go to the `../HTTPServer/bin` directory and issue the command: `./adminctl start`.

Add Web server as unmanaged node

__ 1. After the Deployment manager started, open the Deployment Manager WebSphere Application Server console and add the web server to the cell as an unmanaged node.

__ 2. Open the administrative console at `https://dm&ihs.spnego.company.com:9043/admin`.

__ 3. Go to **System administration > Nodes** and click **Add Node**.

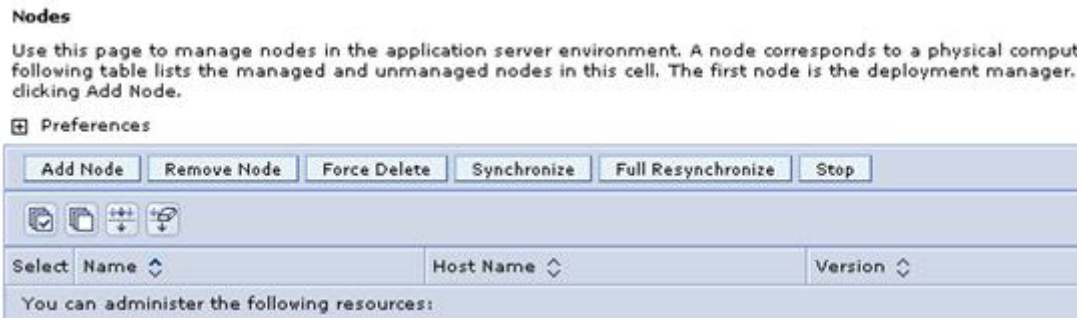


Figure 179. Adding web server as unmanaged node

__ 4. Select “Unmanaged node” and click **Next**.

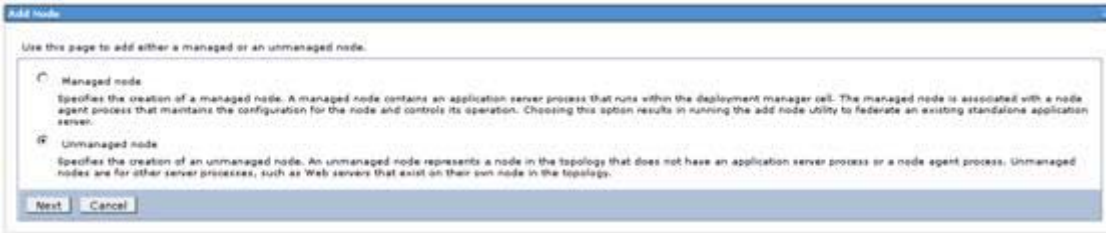


Figure 180. Selecting the option Unmanaged node

__ 5. Provide a name and a host name for the HTTP server and click **OK**.

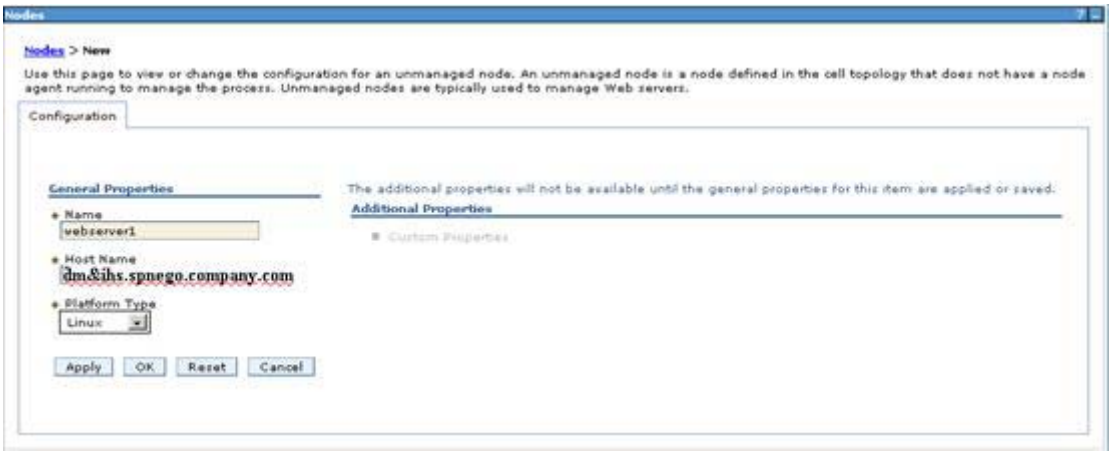


Figure 181. Providing name and host name

__ 6. Click **Save**.

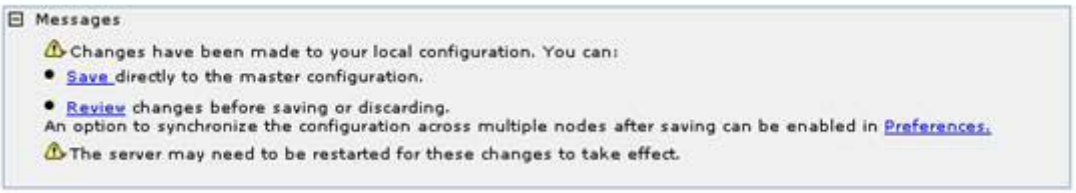


Figure 182. Saving the changes

On the nodes panel, the web server is displayed in the list, as shown in the following figure.

Figure 183. Nodes panel: web server

Add web server as a server

__ 1. Next, go to **Servers** > **Server Types** > **Web servers to** add the web server as a server in the configuration and click **New**.

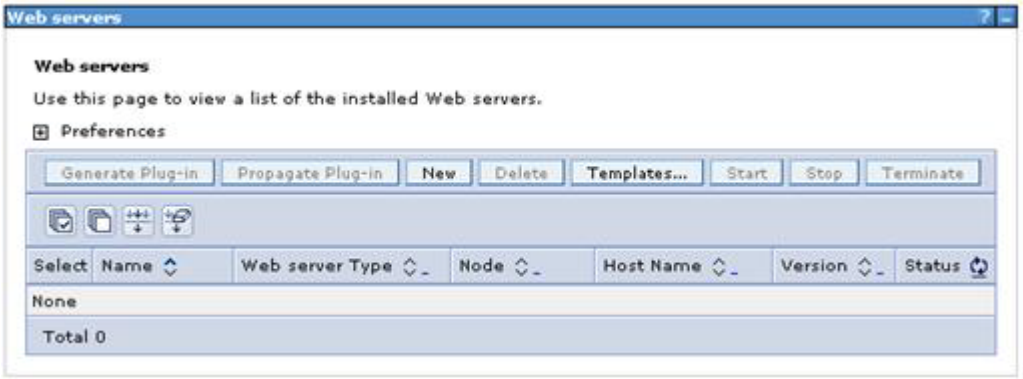


Figure 184. Web servers

__ 2. Select the web server node and provide the name of this server `webserver1`. This is the same name that is provided during the plug-ins installation on the web server.

Type = IBM HTTP Server.

Click **Next** to continue.

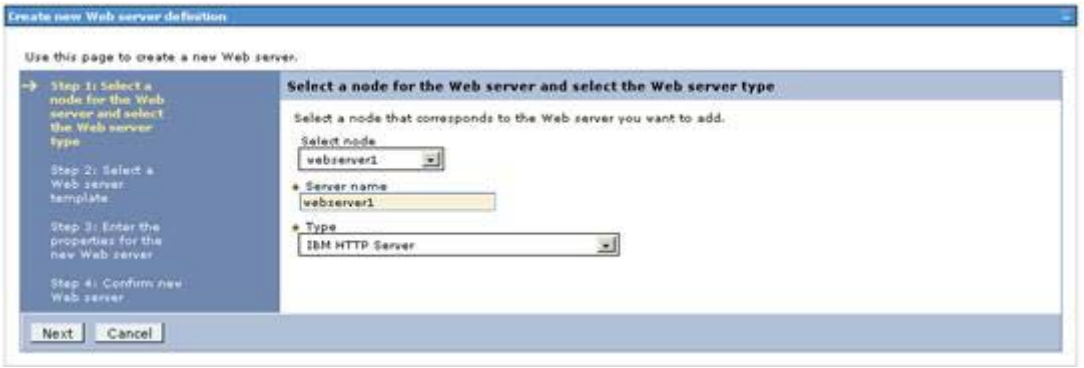


Figure 185. Creating a web server definition

__ 3. Click **Next**.

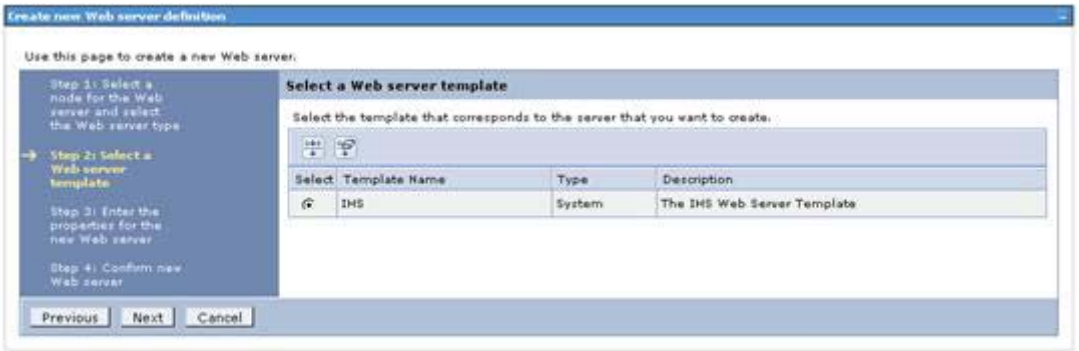


Figure 186. Creating new web server definition

__ 4. Confirm the new web server by clicking **Finish**.

Figure 187. Confirming new web server

__ 5. Select **Save**.

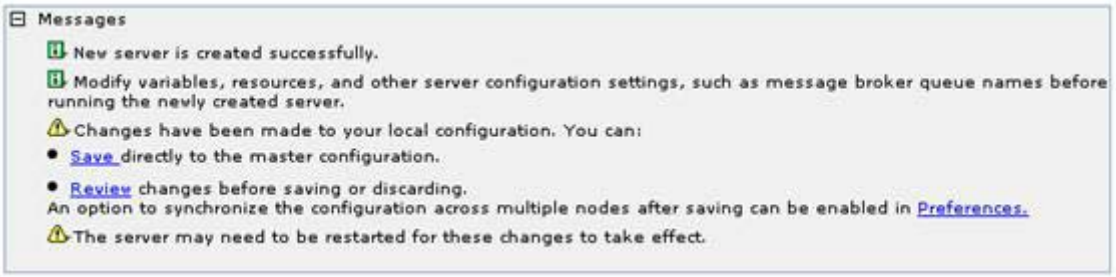


Figure 188. Saving changes

The following screen displays.

Figure 189. The figure shows the created web server

__ 6. Do a **Full Resynchronize** between nodes in the deployment.

Figure 190. Resynchronizing nodes in the deployment

__ 7. Return to **Servers > Server Types > Web Servers**.

__ 8. Select the checkbox next to `webserver1` and click **Generate Plug-in**.

Figure 191. Generating plug-in

The results are as follows:

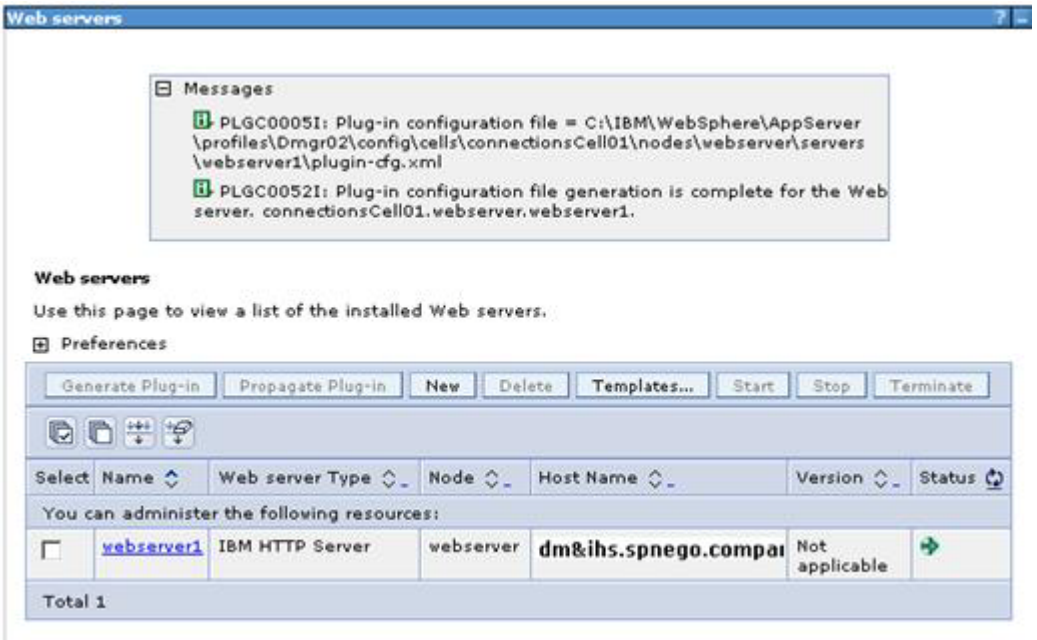


Figure 192. Plug-in generation results

__ 9. Select the check box again and click **Propagate Plug-in** (which propagates the `plugin-cfg.xml` file to the web server).

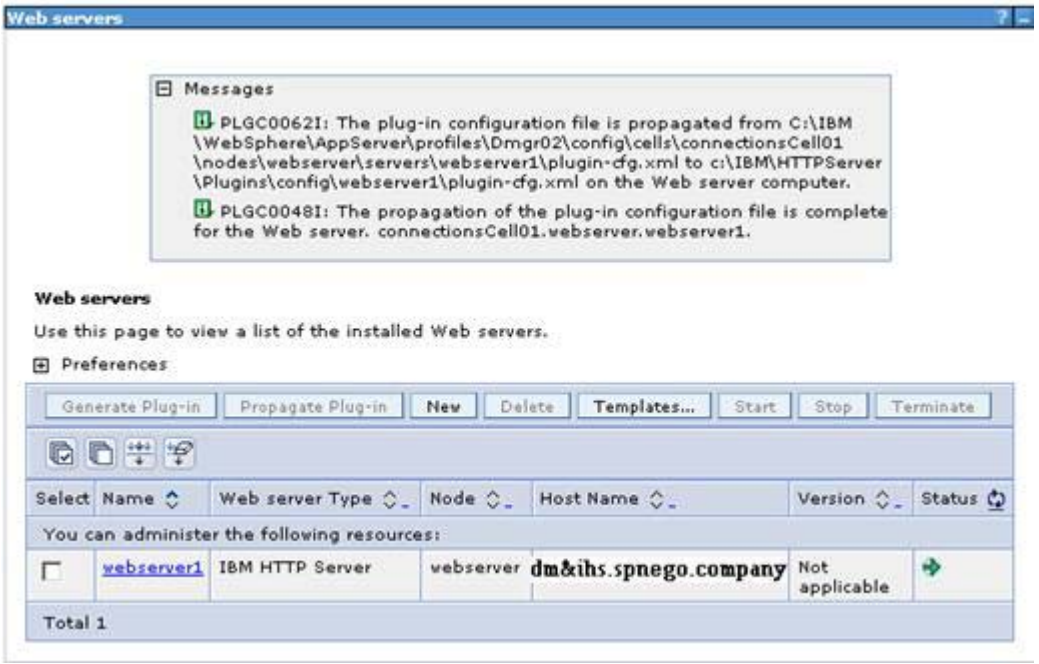


Figure 193. Propagating plug-in

__ 10. Click **webserver1** and then click **Plug-in properties**.

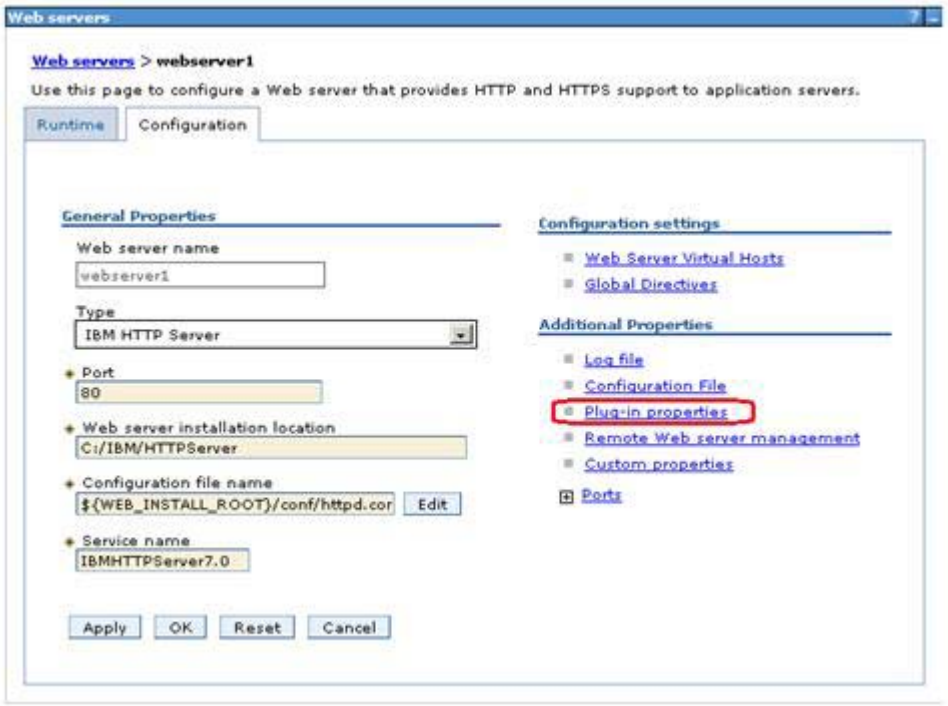


Figure 194. Configuration > Additional Properties > Plug-in properties

__ 11. Click **Copy to Web server key store directory**.

Figure 195. Repository copy of web server plug-in files

__ 12. The following message is displayed to indicate the successful copying of the key files. Once again, restart the web server for the plug-in changes to take effect.

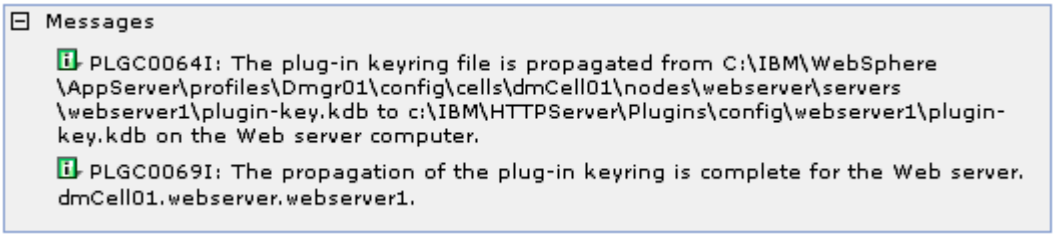


Figure 196. Successful copying of the keys

Configuring IBM HTTP Server for SSL

To support SSL, create a self-signed certificate and then configure IBM HTTP Server for SSL traffic. If you use this certificate in production, users might receive warning messages from their browsers. In a typical production deployment, you would use a certificate from a trusted certificate authority.

__ 1. The first step is to create a key file. Start the iKeyman utility by double-clicking the file `ikeyman.sh` (default dir for this file is `/opt/IBM/HTTPServer/bin`). The following panel is displayed:

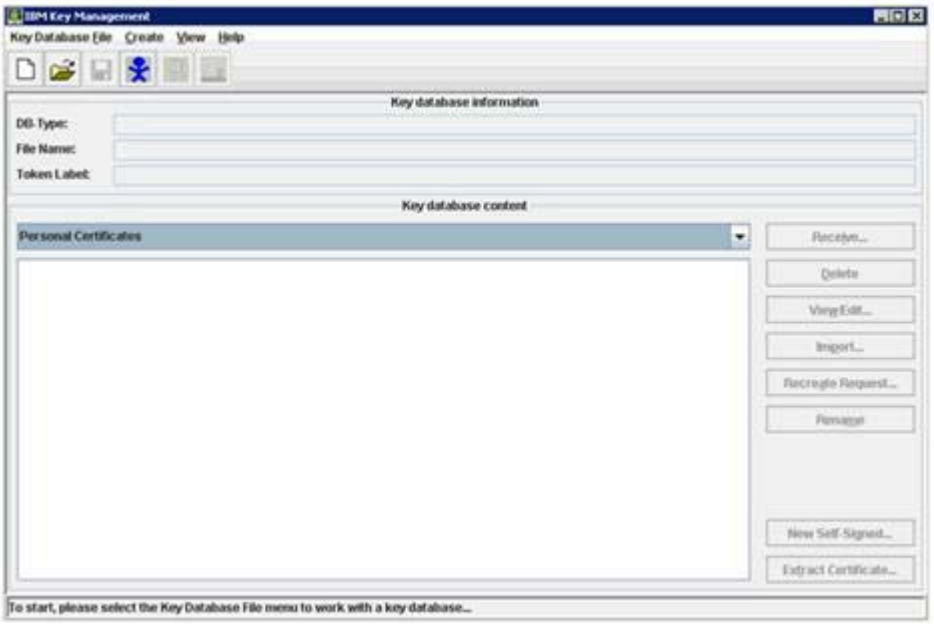


Figure 197. IBM Key Management

__ 2. Click **Key Database File > New...**

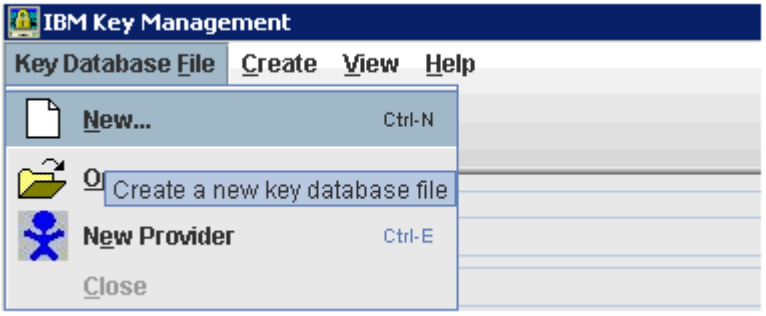


Figure 198. Creating a database file

__ 3. Ensure that the key database type is selected as CMS. Input a name for the key file and location to store it.

Figure 199. Entering type, name, and location for the key database

__ 4. Enter a password and select the **Stash password to a file** option.

__ 5. Click **OK**.

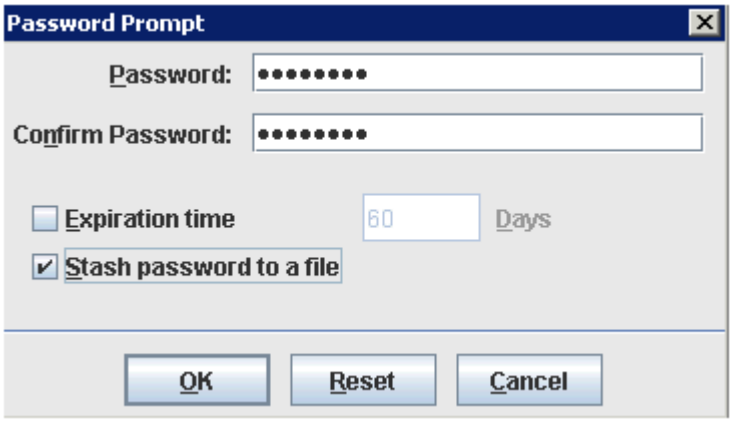


Figure 200. Password prompt

You are then returned to the iKeyman panel with the `webserver-key.kdb` opened.

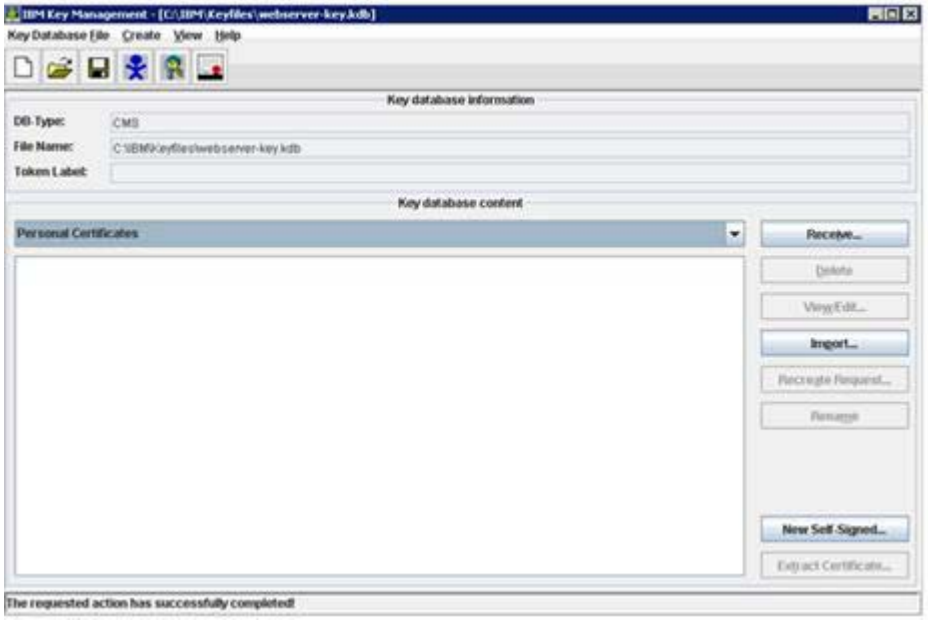


Figure 201. iKeyman panel

__ 6. Now create a self-signed certificate by using **Create > New Self-Signed Certificate**.

Figure 202. Creating a self-signed certificate

__ 7. Input a **Key Label** and the **Common Name**. Click **OK** to save the certificate.

Figure 203. Providing details for the self-signed certificate

The certificate now appears in the key file (note the location of where this file is stored).

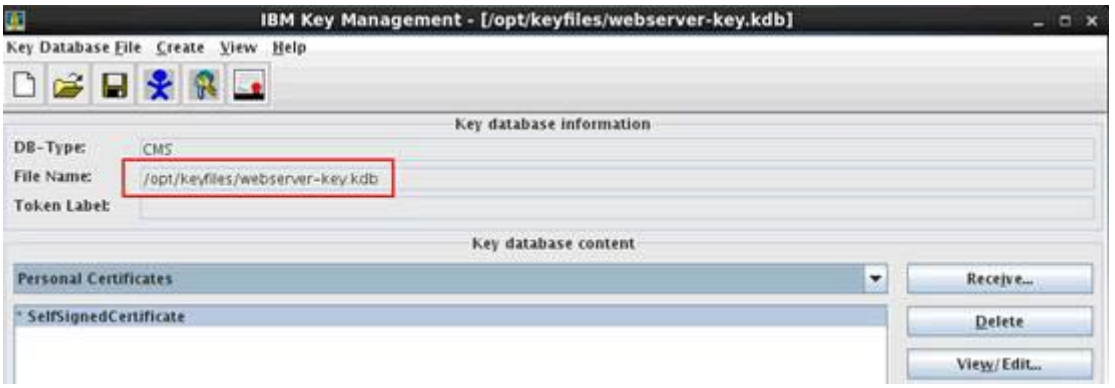


Figure 204. iKeyman: File location

__ 8. Next, in WebSphere Application Server console configure the web server for SSL:

__ a. Stop the IBM HTTP Server.

__ b. Log in to the administrative console and configure the web server for SSL.

__ c. From the Web servers panel, select the `webserver1` link.

Figure 205. Web servers: Configuring the web server for SSL

__ d. Click the **Configuration File** option to open the `httpd.conf` from the administrative console.

Figure 206. General properties: Configuration file

The `httpd.conf` file is displayed.

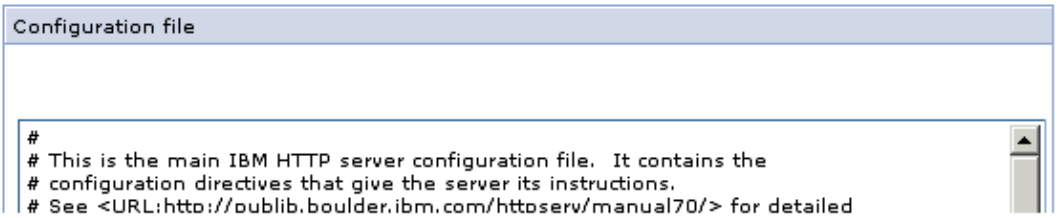


Figure 207. Configuration file

__ e. Add the following lines to the end of the `httpd.conf`:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName dm&ihs.spnego.company.com
SSLEnable
</VirtualHost>
</IfModule>
SSLDisable
Keyfile "/opt/keyfiles/webserver-key.kdb"
SSLStashFile "/opt/keyfiles/webserver-key.sth"
```

__ f. Click **OK** to save this change.

__ g. Next, start the IBM HTTP Server.

__ h. To verify that the SSL settings took effect correctly, type `https://dm&ihs.spnego.company.com` into a browser. If the IBM HTTP Server page appears over https, then this step was successful. You might need to accept the certificate to your browser as it is not signed. Click **Add Exception**.

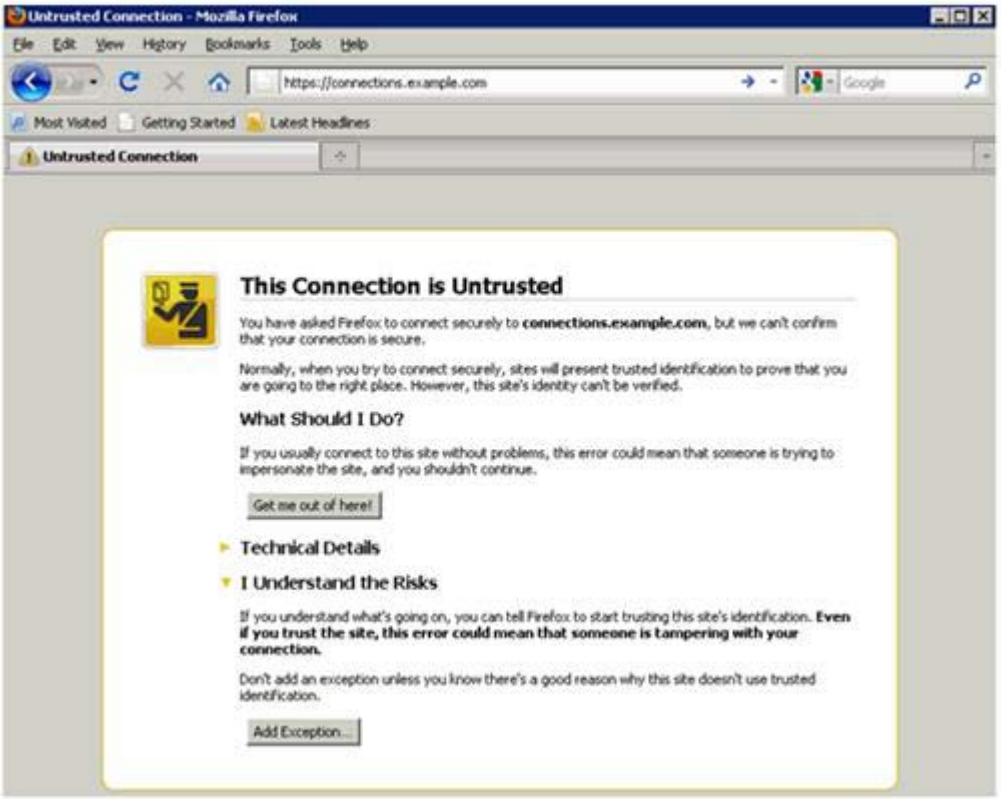


Figure 208. Untrusted connection

__ i. Click **Confirm Security Exception**.

Figure 209. Adding Security Exception

The IBM HTTP Server Version 7.0 home page displays.

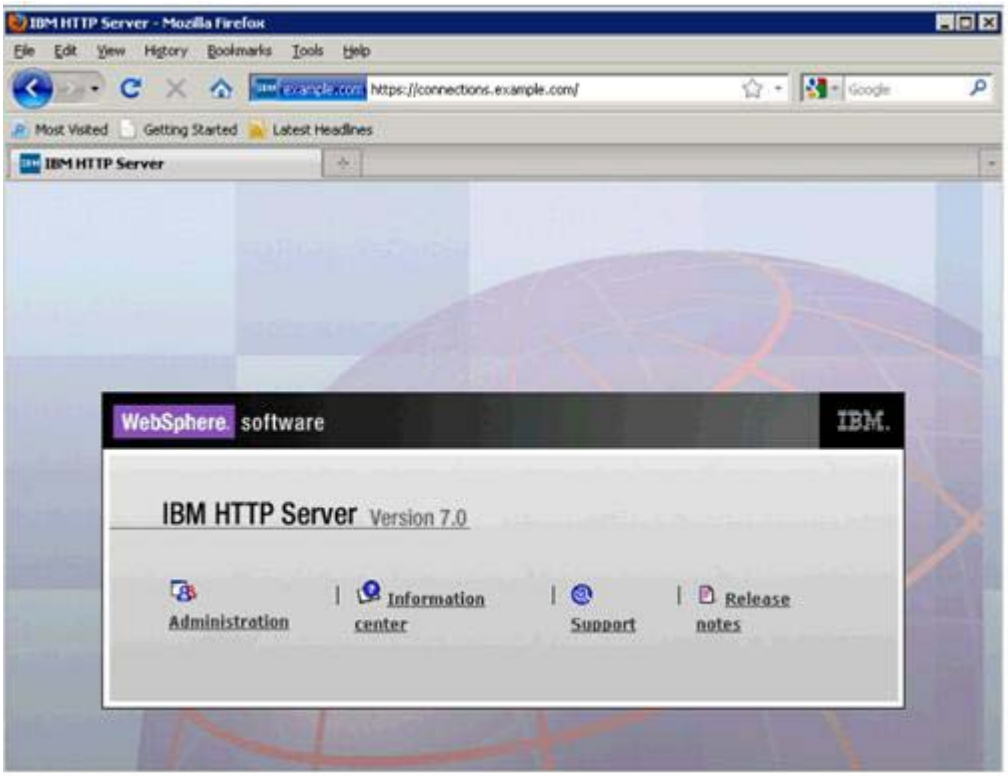


Figure 210. IBM HTTP Server Version 7.0 home page

Adding certificates to the WebSphere truststore

__ 1. On the administrative console go to **Security > SSL Certificate and Key Management > Key stores and certificates**.

__ 2. Click **CellDefaultTrustStore**.

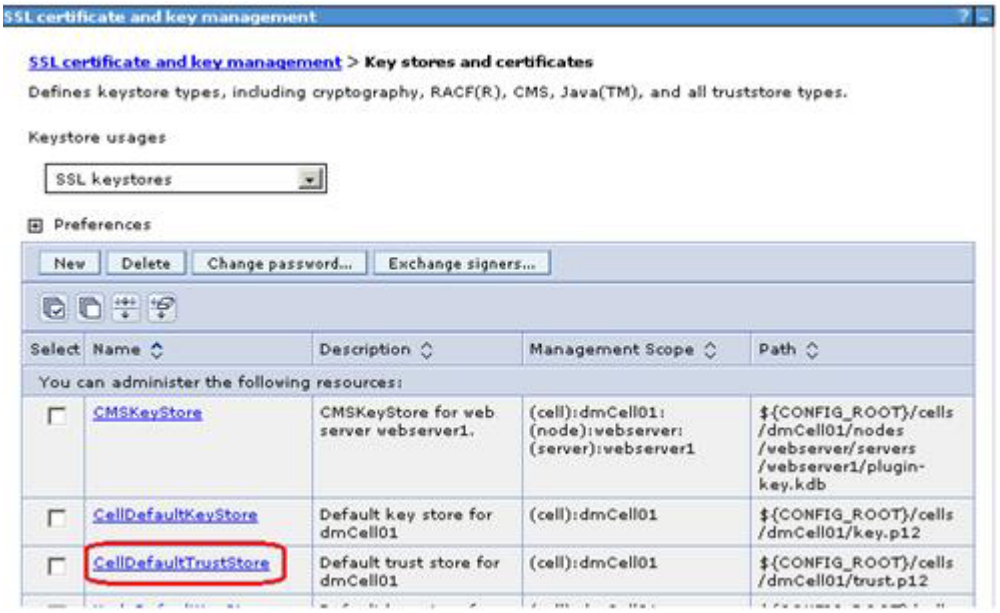


Figure 211. SSL certificate and key management

__ 3. From within **CellDefaultTrustStore**, click the **Signer certificates** link from the right side.

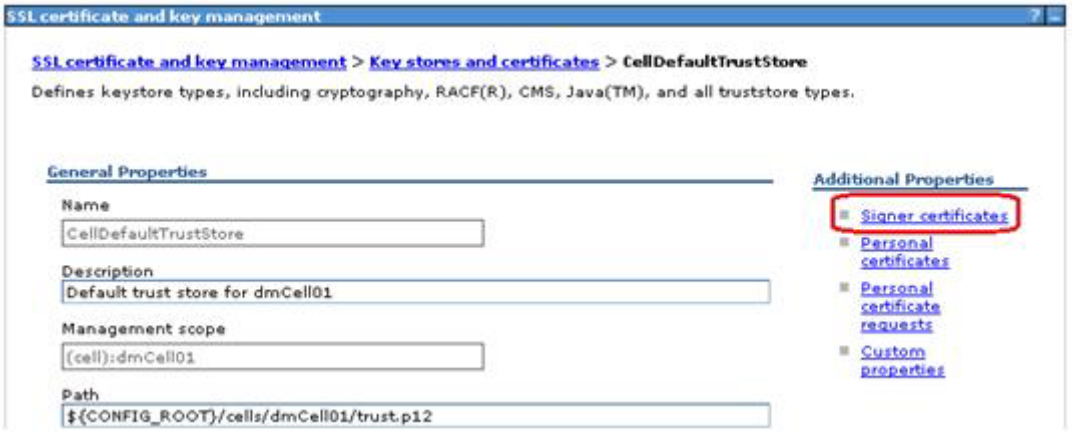


Figure 212. Additional Properties: Signer certificates

__ 4. To add the webservers signer to the truststore, click **Retrieve from Port**.

Figure 213. Retrieving from port

__ 5. Enter the host name of the web server and its SSL port (typically 443) and an Alias.

__ 6. Click **Retrieve signer information**, which retrieves the information that is shown in the following figure.

__ 7. Click **OK** to add this certificate to the list of signers.

__ 8. Click **Save** to save this change.

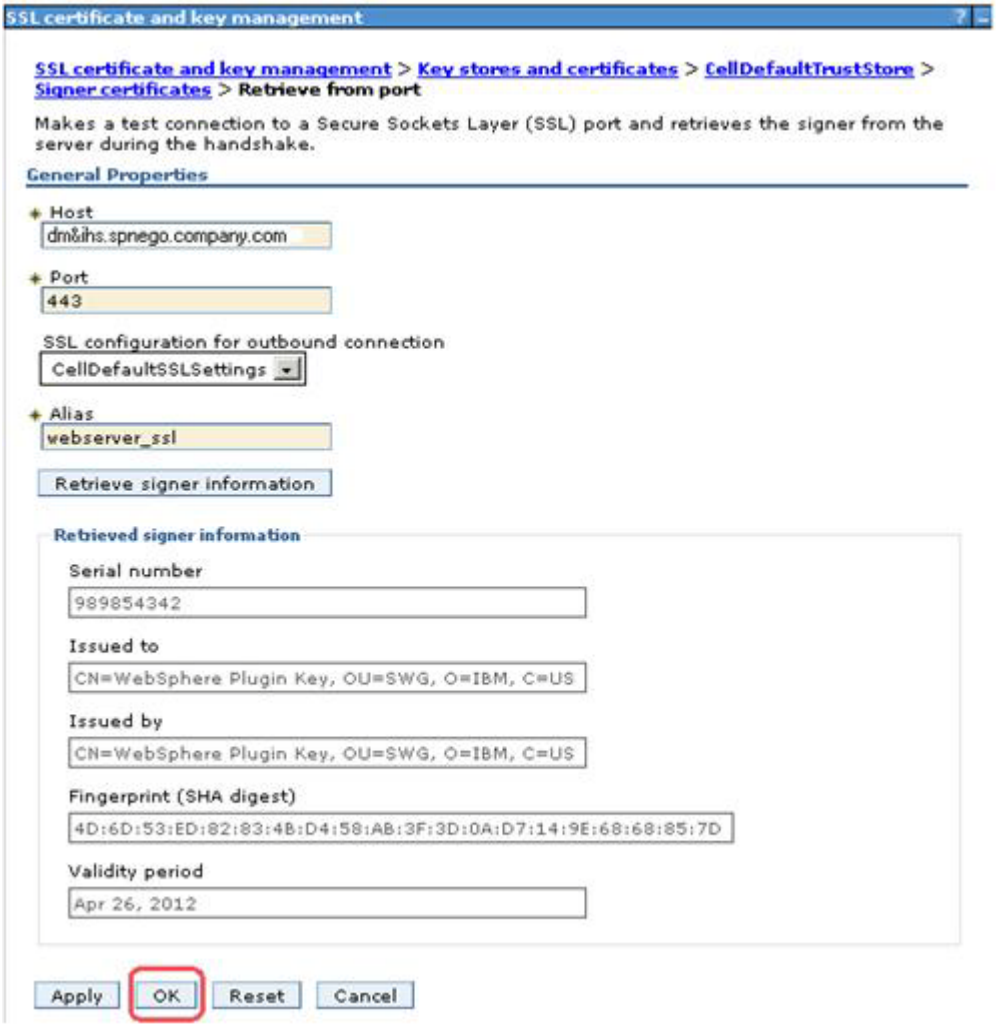


Figure 214. Retrieved signer information

The results are displayed in the following figure.

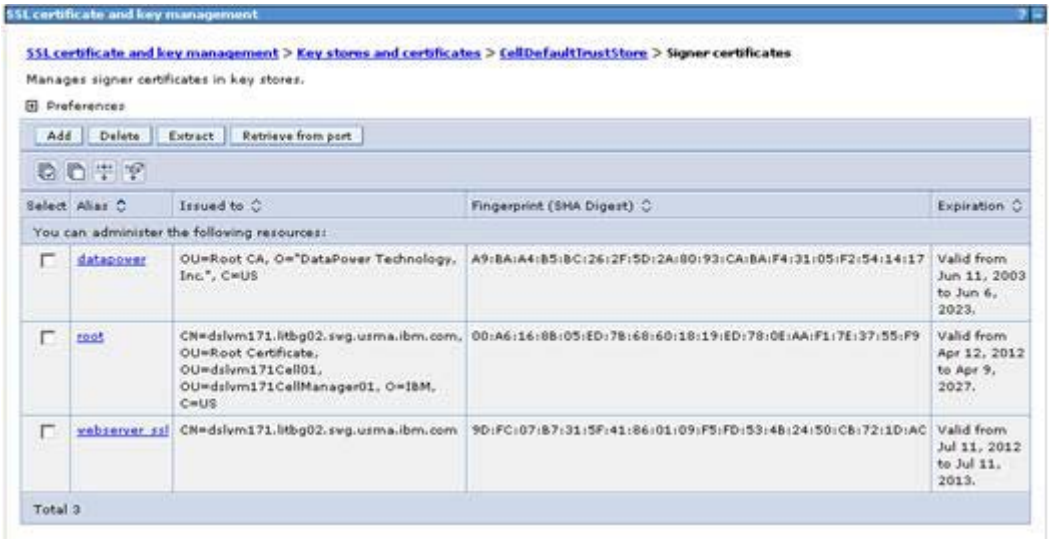


Figure 215. Retrieved signer information results

__ 9. Restart the HTTP server to apply the changes.

Update web addresses used by IBM Connections to access content

__ 1. Using the wsadmin client, check out the `LotusConnections-config.xml` (also known as `lcc.xml`) to a temporary directory. From this directory, this file must be edited so that all `href` and `ssl_href` values are updated to reflect the host name of the HTTP Server and do not include any port numbers. An example of what needs to be done is as follows:

```
<sloc:serviceReference bootstrapHost="connections.example.com" bootstrapPort="2811" clusterName="LotusConnections"
    <sloc:href>
        <sloc:hrefPathPrefix>/activities</sloc:hrefPathPrefix>
        <sloc:static href="http://connections.example.com:9081" ssl_href="https://connections.example.com:9444"/>
        <sloc:interService href="https://connections.example.com:9444"/>
    </sloc:href>
</sloc:serviceReference>
```

Figure 216. LotusConnections-config.xml

__ 2. For each Connections applications, remove the `":"`+`port_numbers` of the two `href` entries and also the `ssl_href` entry.

```
<sloc:serviceReference bootstrapHost="connections.example.com" bootstrapPort="2811" clusterName="LotusConnections"
    <sloc:href>
        <sloc:hrefPathPrefix>/activities</sloc:hrefPathPrefix>
        <sloc:static href="http://connections.example.com" ssl_href="https://connections.example.com"/>
        <sloc:interService href="https://connections.example.com"/>
    </sloc:href>
</sloc:serviceReference>
```

Figure 217. LotusConnections-config.xml

__ 3. Search on `connections.example.com:` and remove the colon (`:`) and the port number. When finished, you should not be able to find any more occurrences of this string `connections.example.com:` (note the colon at the end of the string; this is most important).

__ 4. Save the file and check the file back in using the wsadmin client. After the file is checked back in, resynchronize the node so that this change is pushed out.

__ 5. This completes the web server, SSL, and certificate configuration for this scenario. Now, when the application is started it can be accessed at `http://connections.example.com/<component`, where `<component` represents any of the Connections applications.

The commands to check out and check in the `lcc.xml` file and sync all nodes are as follows:

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>cd C:\IBM\WebSphere\AppServer\profiles\bin
The system cannot find the path specified.

C:\Users\Administrator>cd C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin

C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin>wsadmin.bat -lang jython -usernam
e wasadmin -password wasadmin -port 8879
WASX7209I: Connected to process "dmgr" on node connectionsCellManager01 using SOAP
connector;  The type of process is: DeploymentManager
WASX7031I: For help, enter: "print Help.help()"
wsadmin>execfile("C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\bin_lc_admin
\connectionsConfig.py")
Connections Administration initialized

wsadmin>LCConfigService.checkOutConfig("C:/temp","connectionsCell01")
Connections configuration file successfully checked out
wsadmin>
wsadmin>LCConfigService.checkInConfig()
Using configuration arguments :
        workingDirectory: C:/temp
        cellName: connectionsCell01
        nodeName: None
        serverName: None
Loading schema file for validation: /C:/temp/LotusConnections-config.xsd
Loading schema file for validation: /C:/temp/service-location.xsd
C:/temp/LotusConnections-config.xml is valid
Connections configuration file successfully checked in
wsadmin>
wsadmin>synchAllNodes()
Nodes synchronized
wsadmin>exit

C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin>_
```

Figure 218. Administrator: Command prompt

Configuring an administrator user for blogs

__ 1. Log in to your admin console at `http://dm&ihs.spnego.company.com:9060/admin` (use wasadmin user and password).

__ 2. Select **Application > Application Types > WebSphere Enterprise Applications**, and then select **Blogs**.

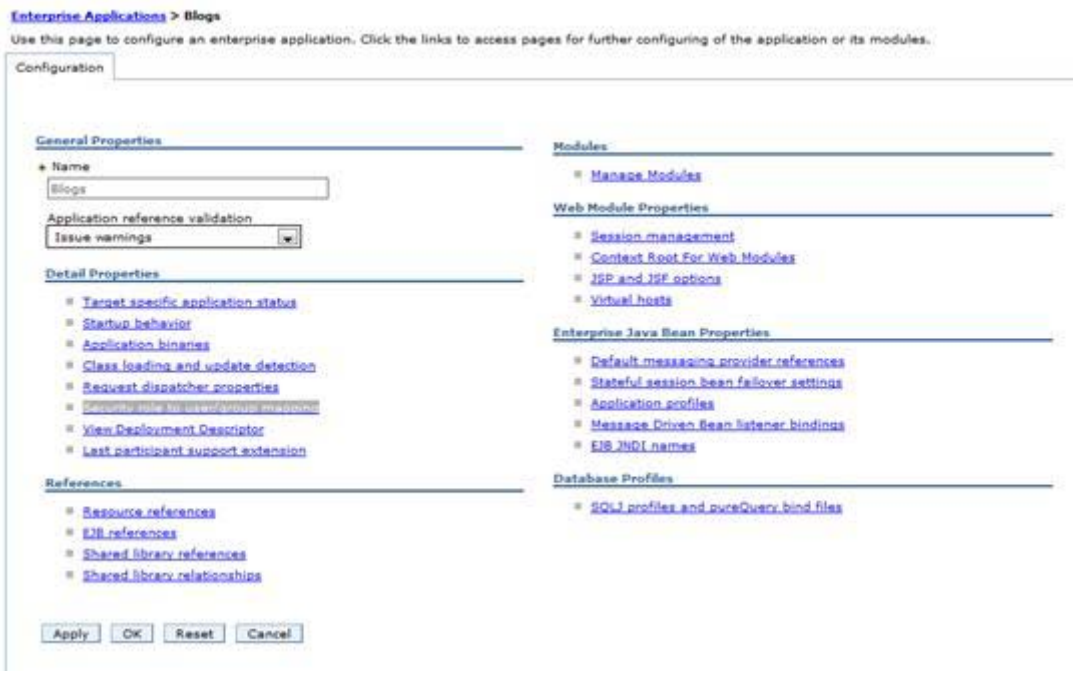


Figure 219. Enterprise Application: Blogs

__ 3. Select **Security role to user/group mapping**.

__ 4. Select the admin role and then **Map Users**.

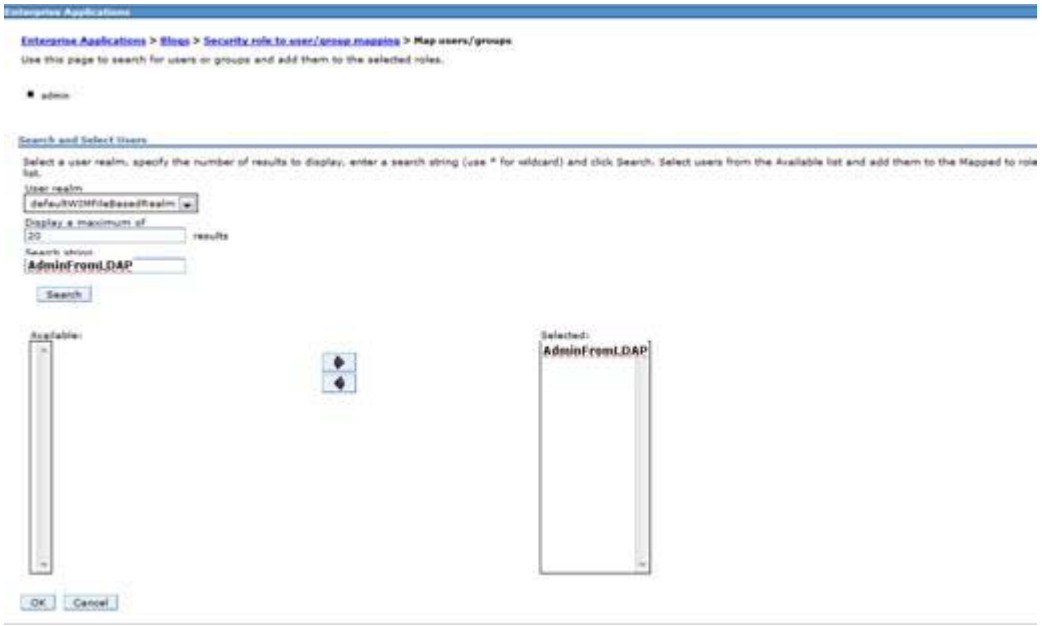


Figure 220. Mapping users

__ 5. Search for the user, **AdminFromLDAP** in this example, and add it.

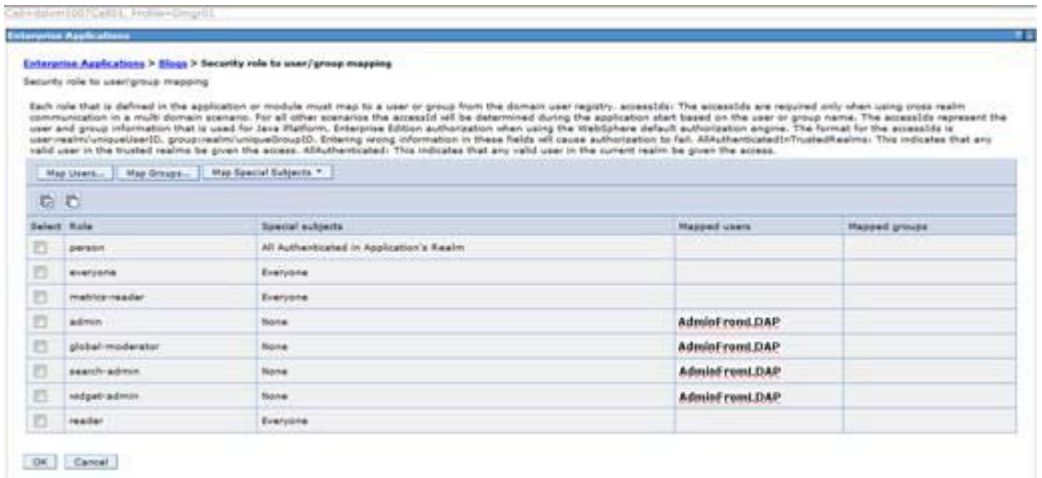


Figure 221. Adding the user

__ 6. Click **OK** and save.

__ 7. Repeat these steps for **home page**.

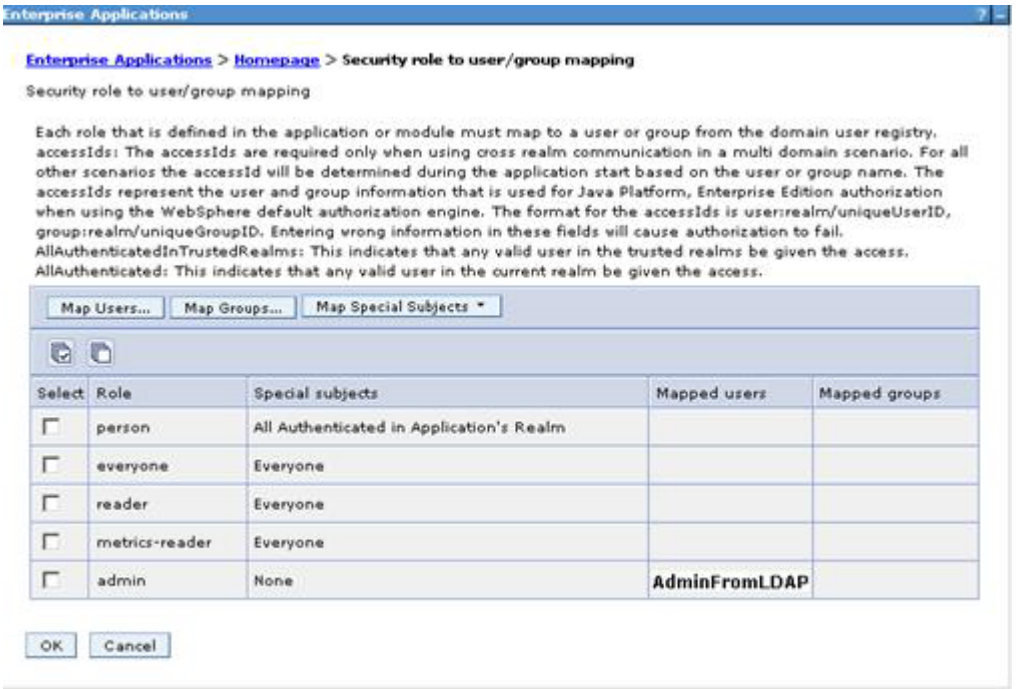


Figure 222. Security role to user/gropu mapping

__ 8. Synchronize your changes with the other nodes.

Enabling fast downloads for files and wikis

Optional

Although this is an optional step for customers, it is dones for all IBM test systems.

__ 1. On the Deployment Manager, copy the file `/opt/IBM/Connections/plugins/ihs/mod_ibm_local_redirect/linux_ia32-ap22/mod_ibm_local_redirect.so` to the IBM HTTP Server system into the folder: `/opt/IBM/HTTPServer/modules/`.

__ 2. cp `/opt/IBM/Connections/plugins/ihs/mod_ibm_local_redirect/linux_x64-ap22/mod_ibm_local_redirect.so /opt/IBM/HTTPServer/modules/`.

__ 3. Edit the `httpd.conf` (/opt/IBM/HTTPServer/conf) and add/edit the following items:

```
LoadModule ibm_local_redirect_module modules/mod_ibm_local_redirect.so
LoadModule env_module modules/mod_env.so
```

Note

These lines might exist, so uncomment if necessary.

__ 4. Add the following to the bottom of the `httpd.conf` file.

Note

Paths must change based on installation.

```
Alias /downloadfiles /opt/IC_Share/files/upload/
 Alias /downloadwikis /opt/IC_Share/wikis/upload/
 <Directory /opt/IC_Share/files/upload/>
 Order Deny,Allow
 Deny from all
 Allow from env=REDIRECT_FILES_CONTENT
 </Directory>
 <Directory /opt/IC_Share/wikis/upload/>
  Order Deny,Allow
 Deny from all
  Allow from env=REDIRECT_WIKIS_CONTENT
 </Directory>
 <Location /files>
  IBMLocalRedirect On
```



```
  IBMLocalRedirectKeepHeaders
X-LConn-Auth,Cache-Control,Content-Type,Content-Disposition,Last-Modified,ETag,Content-Language,Set-Cookie
  SetEnv FILES_CONTENT true
 </Location>
 <Location /wikis>
  IBMLocalRedirect On
  IBMLocalRedirectKeepHeadErs
X-LConn-Auth,Cache-Control,Content-Type,Content-Disposition,Last-Modified,ETag,Content-Language,Set-Cookie
  SetEnv WIKIS_CONTENT true
 </Location>
```

__ 5. On the Deployment Manager, edit the `files-config.xml` and `wikis-config.xml` files that can be found in the folder `/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/config/cells/dslvm171Cell01/LotusConnections-config/` and make the following changes:

__ **a. files-config:**

Search for "<download>" and set the values of the properties to the ones shown in bold:

```
<download>
 <modIBMLocalRedirect enabled="true"
 hrefPathPrefix="/downloadfiles" />
 <stats>
 <logging enabled="true" />
 </stats>
 </download>
```

__ **b. wikis-config.xml:**

Search for "<download>" and set the values of the properties to the ones shown in bold:

```
<download>
 <modIBMLocalRedirect enabled="true"
 hrefPathPrefix="/downloadwikis" />
 <stats>
 <logging enabled="false" />
 </stats>
 </download>
```

__ 6. Synchronize and restart IBM Connections as follows:

__ a. Do a Full Synchronize on all Nodes.

__ b. Stop all Connections clusters.

__ c. Stop and restart the Deployment manager.

__ d. Stop and Restart the HTTP server.

__ e. Start all Connections Clusters.

8. Configuring SPNEGO

Information

Visit `Enabling single sign-on for the Windows desktop` (also known as `Enabling SPNEGO`) in the information center to get more information about this topic.

Configure IBM® Connections to use SPNEGO for single sign-on (SSO). With this configuration, users can sign in to the Windows desktop and automatically authenticate with IBM Connections.

Requirements

In previous steps, you selected a user as an administrator for IBM Connections. You called this user **AdminFromLDAP**. This user must meet the following conditions:

- Is any user from the configured LDAP that you designate as an administrator of Connections.
- Is populated into the `PROFILES` DB.
- Is configured as an Administrator of the Deployment Manager.
- Is select as the Connections administrator during IBM Connections installation.

__ 1. Map an Active Directory account to administrative roles. Change J2C authentication.

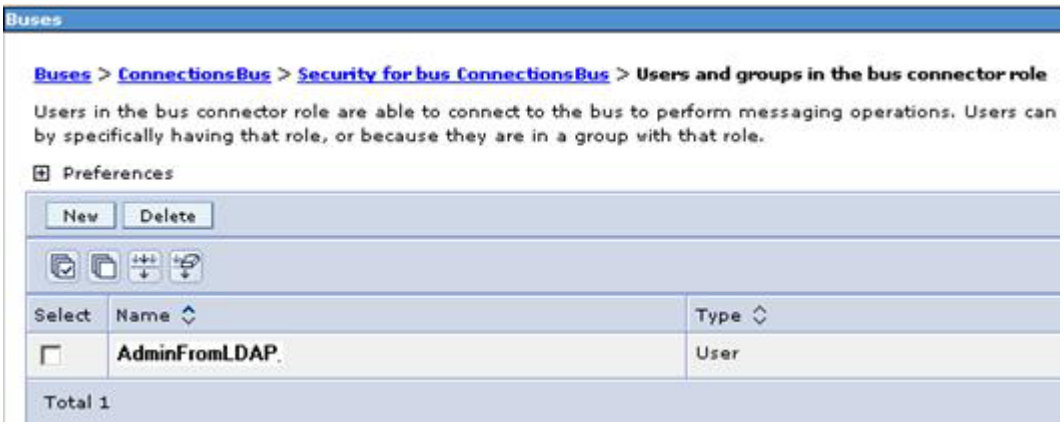


Figure 223. Mapping an Active Directory account to administrative roles

__ 2. Create a service principal name and keytab file.

These steps were performed by the Active Directory Admin who provided the Keytab files for the IBM Connections Deployment Manager, Node1, and Node2.

__ 3. Merge all the keytab files to make the Deployment Manager aware of the SPNs for each node.

The following example demonstrates the procedure for merging keytab files.

Assuming that you created the following keytab files:

__ a. `http.keytab` on the Deployment Manager.

__ b. `krb5Node1.keytab` on Node 1.

__ c. `krb5Node2.keytab` on Node 2.

__ 4. Run the `ktab` command as follows:

```
mkdir /opt/keytab
```

__ 5. Copy the three keytab files into this directory (/opt/keytab):

cd /opt/IBM/WebSphere/AppServer/java/jre/bin

Note

Use this version of ktab and **not** the http version.

./ktab -m /opt/keytab/krb5NodeA.keytab /opt/keytab/http.keytab
./ktab -m /opt/keytab/krb5NodeB.keytab /opt/keytab/http.keytab

__ 6. Verify that all three systems are displayed in the keytab file correctly:

`cat http.keytab` and you should see something like this result:

```
cat http.keytab
SPNEGO.COMPANY.COM HTTP!dm&ihs.spnego.company.com
SPNEGO.COMPANY.COM HTTP!dm&ihs.spnego.company.com
SPNEGO.COMPANY.COM HTTP!node1.spnego.company.com
SPNEGO.COMPANY.COM HTTP!node2.spnego.company.com
```

Figure 224. cat http.keytab

__ 7. Create a Kerberos configuration file named `krb5.conf`:

__ a. Launch wsadmin and create the `krb5.conf` file as follows:

i. cd `/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin`.

ii. ./wsadmin.sh -lang **jacl** -user **AdminFromLDAP** -password **password**.

iii. At the prompt enter:

```
$AdminTask createKrbConfigFile {-krbPath
/opt/IBM/WebSphere/AppServer/java/jre/lib/security/krb5.conf  -realm
SPNEGO.COMPANY.COM  -kdcHost msad2008.spnego.company.com -dns
spnego.company.com-keytabPath /opt/keytab/http.keytab}
```

__ b. Copy the `krb5.conf` file to the `/opt/keytab` folder (which should also have the merged keytab file (`krb5.keytab`)

__ c. Copy this folder and contents into the same location on Node1 and Node2 (i. e. `/opt/keytab folder`)

Note

The location must be the same on all three systems.

```
cat krb5.conf
 [libdefaults]
 default_realm = SPNEGO.COMPANY.COM
 default_keytab_name = FILE:/opt/keytab/http.keytab
 default_tkt_enctypes = rc4-hmac des-cbc-md5
 default_tgs_enctypes = rc4-hmac des-cbc-md5
 forwardable = true
 renewable = true
 noaddresses = true
 clockskew = 300
 [realms]
 SPNEGO.COMPANY.COM = {
 kdc = msad2008.spnego.company.com:88
 default_domain = spnego.company.com
 }
 [domain_realm]
 .spnego.company.com = SPNEGO.COMPANY.COM
```

__ 8. Create a redirect page for users without SPNEGO support.

Use the example that is provided in the information center.

__ 9. Configure SPNEGO on WebSphere Application Server.

__ a. Using the WebSphere Application Server Console and enter the following details:

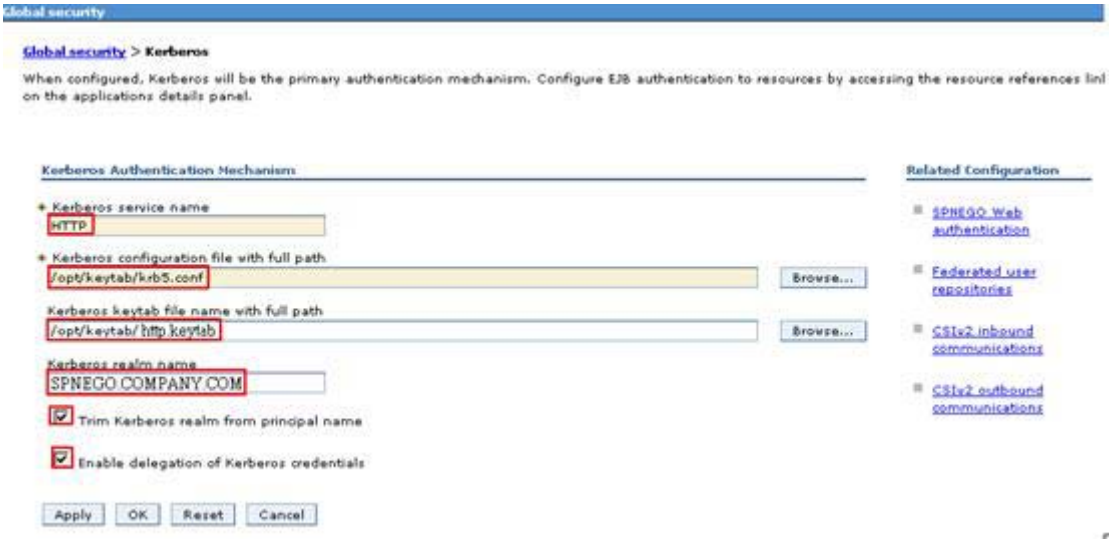


Figure 225. Global security > Kerberos

__ b. Click **OK**, and then **Save**.

__ c. Click **SPNEGO Web authentication** and specify the SPNEGO filter:

i. Under **SPNEGO Filters**, click **New** and populate the dialog as follows:

Note

SPNEGO web authentication and Kerberos authentication use the same Kerberos client configuration and keytab files.

Figure 226. SPNEGO web authentication

__ d. Check the information center for any updates to the Filter criteria. In this example, the following criteria was used:

```
request-url!=noSPNEGO;request-url!=/mobile;request-url!=/nav;request-url!
=/bundles/js;request-url!=/static;request-url!=/activities/oauth;request-
url!=/blogs/oauth;request-url!=/dogear/oauth;request-url!=/communities/ca
lendar/oauth;request-url!=/communities/service/atom/oauth;request-url!=/c
ommunities/service/opensocial/oauth/;request-url!=/communities/recomm/oau
th;request-url!=/connections/opensocial/oauth;request-url!=/files/oauth;r
equest-url!=/forums/oauth;request-url!=/homepage/oauth;request-url!=/metr
ics/oauth;request-url!=/moderation/oauth;request-url!=/news/oauth;request
-url!=/news/follow/oauth;request-url!=/profiles/oauth;request-url!=/wikis
/oauth;request-url!=/search/oauth;request-url!=/connections/core/oauth/;r
equest-url!=/opensocial;request-url!=/resources;request-url!=/oauth2/endp
oint/
```

__ e. On the SPNEGO web authentication page, complete the details for the general properties.

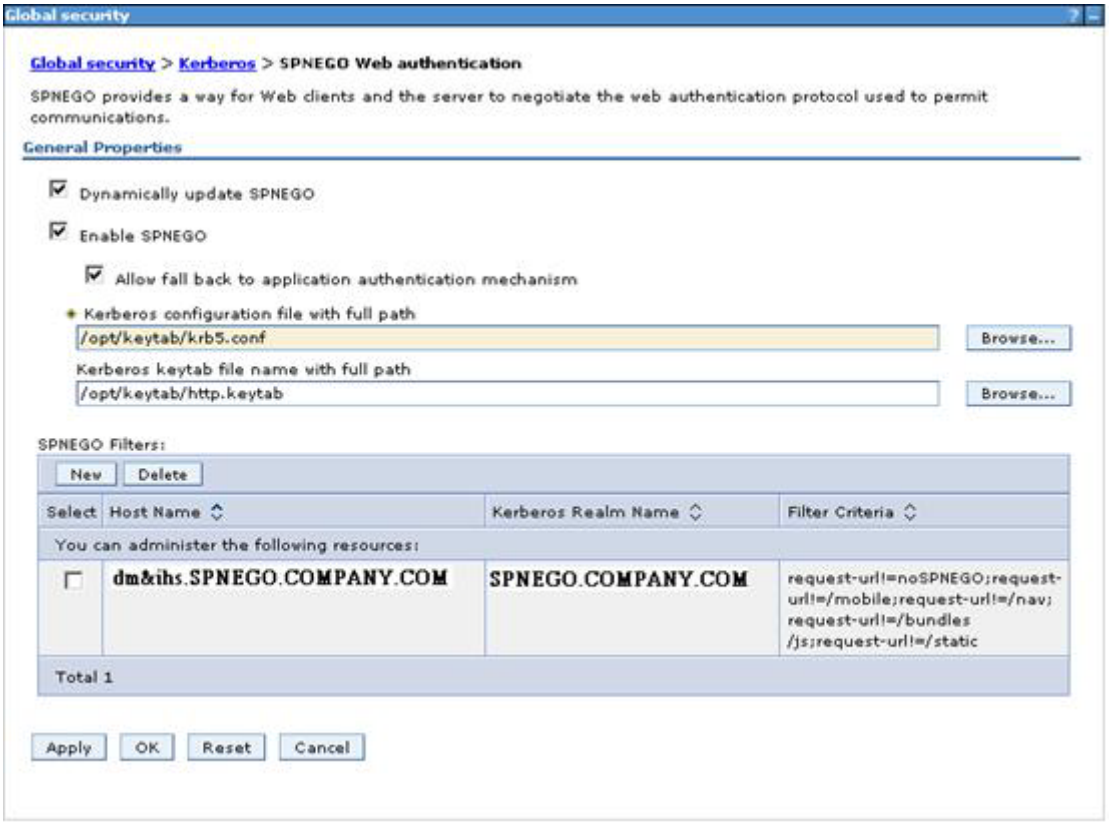


Figure 227. SPNEGO web authentication: General properties

__ 10. Specify the level of authentication that users must go through to access your IBM Connections deployment.

__ a. As this is the setting I want to use in this scenario, there is no need to make any changes here. Allow anonymous access to IBM Connections, also known as Lazy SPNEGO, which is the default.

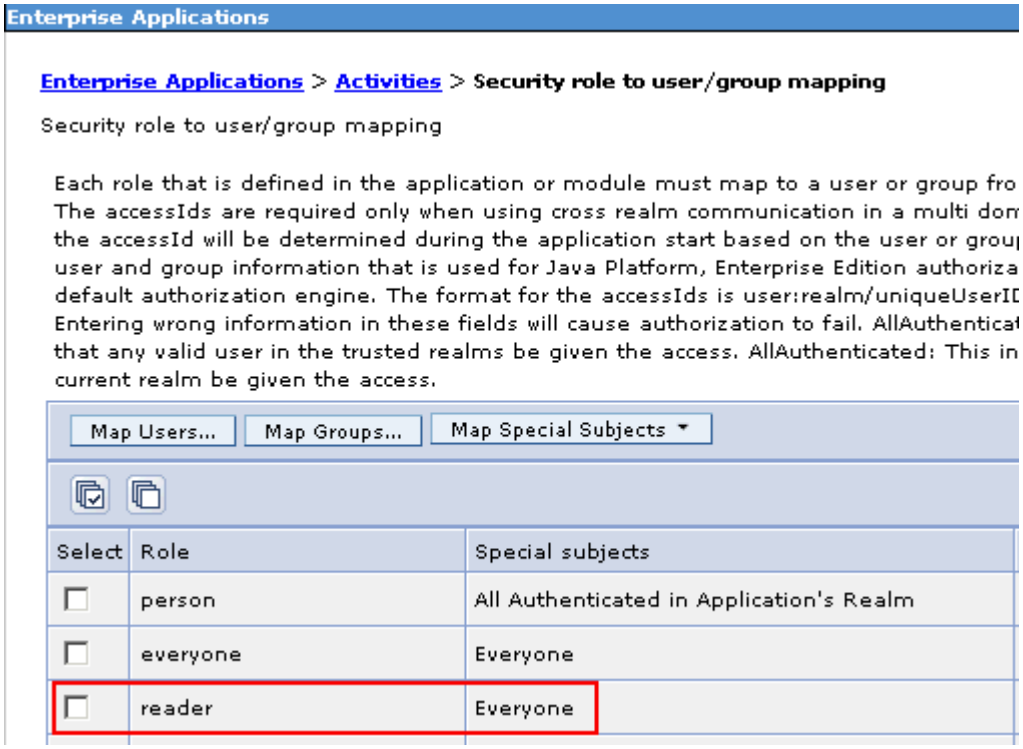


Figure 228. Security role to user / group mapping

__ 11. Remove interceptor classes.

Go to **Security > Global security**, select under “Web and SIP security” the option “Trust association”, then **Interceptors** and remove the following Interceptor Classes:

```
com.ibm.ws.security.spnego.TrustAssociationInterceptorImpl
com.ibm.ws.security.TAMTrustAssociationInterceptorPlus
```

Figure 229. Interceptors

__ 12. Disable TAI authentication:

Select **Security > Global Security > Custom properties > New**.

__ a. NAME: **com.ibm.websphere.security.performTAIForUnprotectedURI**

__ b. Value: **false**

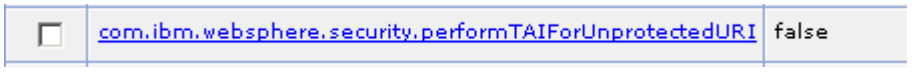


Figure 230. TAI authentication

__ 13. Verify that LTPA is selected as the default Authentication mechanism.

In **Security > Global security**, under **Authentication** verify that **LTPA** is selected as the default for "Authentication mechanisms and expiration". If it is not, then select this option and save.

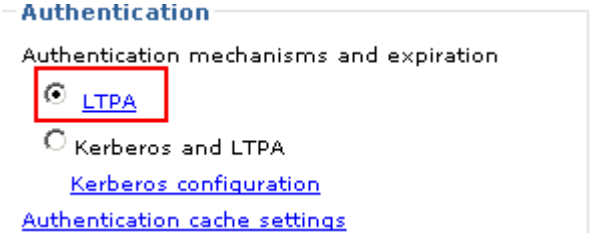


Figure 231. Authentication

__ 14. Edit the following files:

__ a. **files-config.xml**: Set values to `false`.

```
<security reauthenticateAndSaveSupported="false">
<logout href="/files/ibm_security_logout" />
<inlineDownload enabled="false" />
</security>
```

__ b. **LCC.xml (should be already set)**: Verify `customAuthenticator name="DefaultAuthenticator"`.

```
<customAuthenticator name="DefaultAuthenticator"/>
```

__ 15. Stop and restart all server:

__ a. Do a Full Resynchorize of all Nodes.

__ b. In **System administration > Node** agents do a Restart of all nodeagents.

__ c. On the Webserver do a Generate Plug-In and then Propagate Plug-in.

__ d. Stop and restart the webserver.

__ e. Stop all Connections' Clusters.

__ f. Stop the Deployment Manager (`./stopManager.sh`).

__ g. Start the Deployment Manager (`./startManager.sh`).

__ h. Start all Connections' Clusters (this will take a few minutes).

__ 16. Configure a supported web to support SPNEGO.

Information

See “Configuring web browsers to support SPNEGO” in the information center to get more information about this last step.

__ 17. Verify that Connections is correctly configured for SPNEGO as follows:

__ a. Using a supported browser (enabled for SPNEGO), log in to Connections.

__ b. Load all Connections Applications via the navigation menu.

__ c. Create some basis data from each application.

We have now completed the install and configuration of a 2-node cluster of IBM Connections V4, on RedHat Linux 6, with Spnego security enabled.

IBM